1998 - 2009

Una al día

Once años de seguridad informática

Sergio de los Santos
Diseño: Alberto García

Hispasec Sistemas
Seguridad y Tecnologías de la Información

1998 - 2009

Una-al-día

Once años de seguridad informática

versión 2.0

Sergio de los Santos / Diseño: Alberto García

Octubre 2009

Una al día: Once años de seguridad informática
por Sergio de los Santos
Diseño: Alberto García

ISBN: 978-1-4092-4380-9

Descargo de responsabilidad

El libro está basado en su mayoría en información propia de Hispasec, recopilada durante los últimos diez años. Todas las referencias y créditos pueden ser encontrados en la página Hispasec.com. También se ha contrastado información con la Wikipedia en Wikipedia.org, tanto en su versión en castellano como en inglés además de diferentes diarios online.

Hemos tenido el máximo cuidado a la hora de ofrecer datos y fechas, de forma que la información ofrecida sea lo más ajustada y veraz posible. Aun así, no podemos ofrecer responsabilidad ni garantía alguna sobre el contenido del libro.

Con respecto a las erratas, el texto ha pasado varios filtros de corrección, pero es muy probable que no todas hayan sido detectadas y subsanadas. Nos disculpamos de antemano.

Gracias a los que han confiado en mí para llevar a cabo este proyecto, y a todos los que me han ayudado a mejorarlo.

Sergio de los Santos

El libro está estructurado en años. En cada año se hace un recorrido de forma breve por los acontecimientos más importantes ocurridos en la política, sociedad, economía, sucesos... En una segunda sección se habla de los datos y noticias más relevantes ocurridos en seguridad informática en ese mismo año. Se incluyen las mejores una-al-día del año correspondiente, tal cual fueron publicadas, con sus potenciales fallos, erratas, etc. La última sección se trata de una entrevista en exclusiva a los personajes que, por una u otra razón, han sido relevantes en del mundo de la seguridad informática durante el año referido.

Secciones

Durante ese año...

Cada párrafo se corresponde con una breve descripción de los sucesos de cualquier ámbito (ecología, política, sociedad...) que han marcado el año. No pretende ser un exhaustivo anuario que recorra todo lo acontecido en ningún ámbito en concreto, sino un pequeño recordatorio que sitúe históricamente al lector en el contexto del año sobre el que se desarrolla el resto de noticias sobre informática.

Seguridad informática

Cada párrafo se corresponde con una descripción de la evolución de algún suceso destacable relacionado con la seguridad informática. Un recorrido por toda una década de virus, vulnerabilidades, fraudes, alertas e innovación en Internet. En la mayoría de las ocasiones se realiza un pequeño análisis con la perspectiva del tiempo, que ayuda a conocer dónde han ido a parar los proyectos, o qué punto de inflexión supuso el germen de alguna tendencia que hoy en día se conserva.

Una-al-día

Se trata de una pequeña selección de una-al-día. Las que hemos considerado más relevantes y que pueden aportar algo más al apartado previo. Las una-al-día han sido específicamente seleccionadas para ofrecer una visión completa y global de la seguridad del año referido. Suponen un complemento al resumen previo sobre seguridad, ahondado o añadiendo información relevante escrita en el momento del suceso, tal cual se percibía en ese momento. Se ha respetado la ortografía y las potenciales erratas incluso que hayan podido salir publicadas, para obtener una sensación más exacta del contexto en el que fueron escritas.

Entrevista

Hemos realizado entrevistas en exclusiva a los que creemos personajes relevantes de la seguridad: Bruce Schneier, Eugene Kaspersky, Cuartango, Mikel Urizarbarrena, Jorge Ramió, Johannes Ullrich... que nos responden amablemente a preguntas sobre el pasado, presente y futuro de la seguridad informática.

Documentación

Publicaremos algunas fotografías relevantes o anecdóticas sobre Hispasec en estos últimos 10 años.

Todo el texto está salpicado además de pequeñas y grandes anécdotas referentes a una-al-día e Hispasec, secretos confesables y documentación añeja.

Índice - Resumen

Comienzan a publicarse las una-al-día. Es el año de los agujeros de Cuartango y Guninsky, de la aparición de Windows 98 sin ningún concepto de seguridad y su juicio antimonopolio, de la creación del ICANN, del nacimiento de Google, del virus Chernobyl... de una Internet plagada de molestos popups y páginas estáticas, de pleno auge de la burbuja "puntocom" y de velocidades de 33.600 bps.

Es el año de Napster, Netscape, de la especulación en torno a la burbuja "puntocom", de las empresas creadas sólo con ideas y acciones infladas, del gusano Melissa y los virus de macro, del miedo ante el efecto 2000, de los dialiers y las tarificaciones abusivas, de decenas de ISPs que regalan Cds para configurar conexiones con coste de llamada metropolitana, de los portales multidisciplinares desde donde se "accede a Internet"...

Prólogo a la edición anterior

Hace un año, por estas mismas fechas cumplíamos 10 años, motivo por el cual nos embarcábamos en el apasionante reto de la publicación de un libro que recogiera todo lo acontecido en esos 10 años, en el mundo de la seguridad informática. A la larga el proyecto se convirtió en algo mucho más ambicioso, dando como resultado un magnifico volumen en el que se hacía un recorrido por 10 años de historia, de informática, de seguridad informática, de curiosidades sobre Hispasec y se complementaba con un buen número de entrevistas a personas relevantes de nuestro sector.

Ha transcurrido un año más, por lo que si Pitágoras no falla ahora cumplimos 11 años, un número menos redondo pero no por ello menos importante. De una forma mucho más silenciosa, pasando desapercibida, hace pocos días enviábamos la "una al día" número 4.000. Para no sobrecargar a nuestros lectores con múltiples avisos y celebraciones de aniversario preferimos juntar todo en una única fecha.

Por todo ello, editamos ahora una nueva versión de nuestro libro, con una revisión y ampliación para cubrir todo lo acontecido durante este último año, para además publicarlo en formato digital.

Este último año no ha estado exento de grandes retos y emociones para Hispasec Sistemas. La concesión del "Trofeo Extraordinario del Jurado" dentro de los "Trofeos de la Seguridad TIC 2008" de la revista Red Seguridad, la cada vez mayor repercusión de VirusTotal internacionalmente, la ampliación de recursos en VirusTotal, la ampliación de nuestro laboratorio técnico o nuestra participación como miembros fundadores del Consejo Nacional Consultivo de CiberSeguridad...

Aun con todo, el prólogo que tuve ocasión de escribir el año pasado sigue totalmente vigente por lo que antes de ofrecer la introducción del pasado año, no me queda más que reiterar el agradecimiento a todos los que hicieron y han hecho posible Hispasec y este libro, a los amigos, lectores, integrantes y clientes de Hispasec.

Antonio Ropero

Introducción

Hace diez años no había mucha información sobre seguridad informática que fuera más allá de los virus del momento. Internet tampoco estaba muy implantado en la sociedad como ocurre en la actualidad. Sin embargo hace diez años, hablando por IRC con Bernardo, me dijo algo así como “apuesto a que hay suficiente material sobre seguridad como para sacar una noticia todos los días”. No me sorprendió.

En aquella época yo trabajaba en la revista PC Actual y Bernardo era colaborador externo. Solíamos redactar juntos artículos sobre temas de seguridad, comparativas antivirus, y similares. Así que escribir sobre informática, o en concreto sobre seguridad informática, no nos resultaba raro ni complicado.

Bernardo escribió ese mismo día la primera noticia y la envió a un pequeño grupo de amigos y compañeros. El reto propuesto por Bernardo me pareció una gran idea, además tenía claro que era totalmente factible, así que me propuse ayudarle con otra noticia. Los dos primeros días, Bernardo envió su noticia, pero al tercero envió la que había escrito yo. Poco a poco, se convirtió en algo habitual, entre los dos y sin darnos apenas cuenta habíamos conseguido mantener el ritmo diario.

De esa forma tan espontánea nació una-al-día y el proyecto empezó a tomar forma y a ampliarse. Habíamos conseguido mantener la regularidad día a día, y cada vez era más gente la que nos pedía que le añadiésemos a la lista de los que recibían la noticia. En las primeras semanas del proyecto también se unieron Antonio Román y Jesus Cea, de forma que lo que hoy es Hispasec empezó a convertirse en realidad. Trabajamos en un diseño y dos meses después, a finales de 1998, nacía el portal de Hispasec.

Cada día se apuntaba más gente y en pocos meses ya contábamos con miles de subscriptores. Con el tiempo, la aceptación del servicio creció hasta sobrepasar los 40.000 suscriptores diarios directos, y sobre todo, comenzamos a ser reconocidos como una fuente de información rigurosa sobre seguridad informática con un carácter técnico y total independencia de terceros.

Hispasec había nacido como un reto desinteresado, sin ninguna pretensión económica ni empresarial, pero la demanda de los propios usuarios y lectores hizo que el proyecto se afianzara y dos años más tarde nació Hispasec Sistemas. Una empresa creada y gestionada por los cuatro fundadores de Hispasec, con el mismo carácter con el que había nacido una-al-día. Es decir, una empresa de marcado carácter técnico, sin capital externo, total independencia de intereses ajenos y pensando en seguir ofreciendo servicios a la comunidad.

Desde un primer momento Hispasec se vio envuelta en continuos proyectos, mejoras y crecimiento. Pero aun con la gestión empresarial de por medio, siempre hemos mantenido nuestra primera idea de ofrecer servicios gratuitos que sirvan para mejorar la seguridad e información de la comunidad: una-al-día, CheckDialer, informes técnicos, VirusTotal y su VTUploader, y muchos otros. Y esperamos, con la ayuda de todos, poder seguir haciéndolo durante mucho tiempo más.

Más de 3.650 una-al-día publicadas hasta la actualidad, seleccionar un grupo de ellas (86 en concreto) es un difícil reto. ¿Qué criterios seguir para la selección? No quiere decir que sean las mejores noticias del año, ni las que más repercusión hayan tenido. Seguramente nuestros lectores más habituales recuerden alguna en especial que no aparezca. Una labor de selección complicada, realizada pensando en tratar de ofrecer una visión global de la seguridad en el año concreto.

Pero hemos querido ir mucho más lejos. Este libro, no es solo una selección de las una-al-día publicadas. El estupendo trabajo realizado por Sergio de los Santos permite tener una idea general del estado del mundo

en sus aspectos más globales (política, sociedad, etc.), de la informática y concretamente de la seguridad informática. Permite recapitular los detalles más relevantes de cada año, recordar sucesos ya olvidados, y englobar cada año en su contexto. Para ello, en cada uno de los once capítulos en que se estructura este libro, se realiza un breve recordatorio de los hechos sociales, políticos, económicos del año, y un repaso de datos y sucesos más relevantes en relación con la seguridad informática.

Además cada capítulo se ve complementado con una entrevista a diez personajes representativos de la seguridad informática en España y en el mundo. Bernardo Quintero se ha encargado de formular unas interesantes preguntas a Bruce Schneier, Kaspersky, Cuartango, Mikel Urizarbarrena, Jorge Ramió, Mercé Molist, Juan Salom, Hector Sánchez Montenegro y Johannes Ullrich. Todos ellos dan su visión sobre la seguridad informática, cómo ha cambiado o evolucionado a lo largo de estos últimos diez años, qué nos depara, o cómo ha sido su relación con Hispasec. Nuestro más sincero agradecimiento a todos ellos por su colaboración en este proyecto.

Los más fieles seguidores de una-al-día, que nos consta que los hay, también encontrarán múltiples curiosidades a lo largo del libro. Hemos rebuscado en los cajones, en copias de seguridad ya olvidadas, en carpetas olvidadas en discos duros y entre los mensajes más antiguos para ofrecer datos y fotografías nunca antes revelados ni publicados sobre Hispasec.

En estos 10 años todos hemos sufrido muchos cambios, y este libro bien refleja todos ellos, tanto en la sociedad como en el mundo de la informática. A modo de reflexión, se podría decir que en muchos aspectos la seguridad informática ha cambiado bien poco. Para muchas empresas sigue siendo una carga, y muchas otras no ven la necesidad de invertir en seguridad hasta que no ven las “orejas al lobo”. Por otra parte, el eslabón más débil en la cadena de la seguridad informática sigue siendo el usuario. En eso no hemos cambiado.

Sólo me queda aprovechar la ocasión para agradecer a todos los que en algún momento, de una forma u otra, han dado lugar a que el espontáneo proyecto original se haya convertido en la actual Hispasec. Bien por su aportación, confianza, enseñanzas o sugerencias e incluso críticas. A PC Actual (y todos sus integrantes), a los subscriptores de una-al-día, a todos los que hayan leído alguna de nuestras informaciones, compañeros, clientes, a los usuarios de cualquiera de nuestros servicios.

Muy especialmente a:

Francisco Santos, Julio Canto, Sergio de los Santos, Eusebio del Valle, Giorgio Talvanti, Xavier Caballé, Sergio Hernando, Javier Labella, Santos Herranz, Esther de Pazos, Karim Adolfo Bouhlala, Moritz Konstantin Meurer, Pablo Molina, David García, Emiliano Martínez, Michael Skladnikiewicz, Alberto García, Pawel Janic, Alejandro Bermúdez, Manuel Castillo, Victor Manuel Álvarez, Marcin Noga, Matthew Jurczyk, María del Carmen Padilla, Christian Soto, Rafael Fuentes, Jacob Fernández, Carlos Boni, Victor Torre, David Reguera, Alejandro Gómez, José Ignacio Palacios...

...y todos los que lo han hecho realidad.

Antonio Ropero: Socio fundador de Hispasec

7CE

3716

Capítulo 0

AÑO 1998

11111001110



883612800 – 915148799



Durante este año...

_ El año comienza con el fenómeno meteorológico de **El Niño** en todos los informativos. Las tormentas causadas azotan el norte de América y meses más tarde, se cebaría en Florida con una nueva ola de tornados. El nombre de “El Niño” viene de “El niño Jesús” por anunciarse habitualmente en la época de Navidad en la costa oeste de América del Sur. Aunque los efectos de este fenómeno ya se descubrieron en 1923, fue mundialmente conocido durante ese año.

_ La película **Titanic**, estrenada el año anterior, gana 11 premios de la Academia (Oscars). James Cameron consigue así un rotundo éxito de taquilla tras Terminator 2 en 1991. El director rodó casi consecutivamente dos de las películas más caras de la historia: Terminator 2 y Titanic. Terminaron por ser tan caras como rentables.

_ En marzo se descubre que **Galileo**, la sonda enviada al espacio, ha recopilado datos que indican que la luna Europa del planeta Júpiter podría disponer de un océano líquido bajo una capa de hielo.



_ La administración americana aprueba la **Viagra** como medicamento para tratar la impotencia. Esta pastilla se convertiría en un pequeño milagro azul para miles de hombres y más tarde, en un potente reclamo en el correo basura. Su precio es elevado, y existen decenas de farmacias clandestinas en Internet destinadas a la producción (de forma legal o no). En ocasiones se trata de una estafa, en otras permiten adquirirla de forma barata y anónima. El correo basura, durante mucho tiempo, tendría en la Viagra (y todas sus variantes ortográficas posibles) su mayor aliado.

_ El 25 de abril se rompe la presa de contención de la balsa de la mina de pirita en **Aznalcóllar** (Sevilla). Se vierte agua ácida y lodos muy tóxicos en 100 kilómetros cuadrados, constituyendo un gravísimo desastre ecológico que afecta a la reserva del Coto de Doñana. Las organizaciones ecológicas pregonan que era un desastre anunciado, y hoy día siguen diciendo que es posible que vuelva a ocurrir. La causa penal sería archivada en 2001. Diez años después no se ha castigado a ningún responsable del desastre.

_ Eurovisión, el festival caduco y desfasado (que sufriría una revitalización en 2001 gracias a Operación Triunfo) nombra a un transexual como ganadora, **Dana International**. A pesar de su efímera fama, la artista lleva 14 años trabajando.

_ Se acuñan ya las **primeras monedas de Euro**, tras un primer intento de introducción del ECU como moneda “abstracta”. Las especificaciones finales no fueron emitidas hasta finales de año, con los que todas estas primeras monedas tendrían que ser fundidas y vueltas a hacer en 1999.

_ Charlton Heston se convierte en presidente de la controvertida **National Rifle Association** (Asociación Nacional del Rifle), una organización que defiende el derecho libre de la tenencia de armas de fuego. En 2003 Michael Moore le haría partícipe involuntariamente de su película-documental Bowling for Columbine. Aunque Moore consiguió un importante golpe de efecto, también sería criticado por “manipular” a Heston. El actor moriría en 2008 víctima de una enfermedad degenerativa. Defendió la igualdad de derechos civiles entre blancos y negros en Estados Unidos durante los años 60.

_ En el mundial de fútbol de Francia de ese año, **España no pasa ni a octavos**. Es derrotada en la primera fase contra Bulgaria, Paraguay y Nigeria. Pasarían diez años para que se resarciese y ganara la copa de Europa de 2008.

_ Durante todo el año, el escándalo de **Bill Clinton y Monica Lewinsky** está en su mayor apogeo. Nunca una felación había proporcionado tanto rédito. Los primeros rumores e informaciones sobre este asunto fueron volcadas en Internet. Al parecer la becaria de la Casa Blanca, de 25 años entonces, había mantenido “relaciones sexuales” con el presidente de Estados Unidos (Clinton sostuvo durante mucho tiempo que no mantuvo relaciones con esa mujer, por no considerar el “sexo oral” como una “relación”). Matt Drudge, responsable de la página “The Drudge Report”, fue el primero en difundir el escándalo, que costó algún tiempo publicar en medios serios por la “gravedad” del asunto. Monica publicaría muy poco después, en 1999, un libro llamado “Monica’s Story”, una biografía autorizada en la que detallaba su affair con Bill Clinton. Hoy tiene su propio negocio y vende su propia marca de bolsos, además de aparecer ocasionalmente en programas de televisión.



_ El británico Kevin Warwick realiza las **primeras pruebas de implantación de RFID** (Radio-frequency identification) en humanos, insertando un chip en su propio brazo. RFID es una tecnología destinada a identificar cualquier objeto o animal a través de un dispositivo equipado con una antena y un chip que almacena información. Da pie a un abierto debate sobre el asalto a la intimidad que podría suponer la identificación de personas y los posibles problemas de seguridad que sufriría el protocolo o la implementación. Es considerado un serio atentado contra la privacidad. Se le llega a llamar “código de barras para humanos”. En Florida, una familia entera (los Jacbos) se implantarían chips RFID en febrero de 2002. Su intención sería la de almacenar en ellos información médica importante que pudiera ayudarles o prevenir problemas de contraindicaciones con medicamentos en situaciones de emergencia.

_ El Reino Unido se despide parcialmente de **la pena de muerte**. Se ratificó así la convención de Derechos Humanos prohibiendo la pena de muerte excepto en “tiempos de guerra o inminente amenaza de guerra”. Dejando una puerta abierta para aplicar el castigo. Habría que esperar a febrero de 2004 para que quedase prohibida definitivamente bajo todas las circunstancias.

A mediados de 1998, la configuración estándar de un sistema podía ser:

Precesador Pentium II a 350 MHz, 64 Megas de SDRAM a 100 Mhz, Disco duro de 4.3 Gigabytes, VGA de 8 megas, Monitor CRT de 17 pulgadas, CD ROM de 32 velocidades, SoundBlaster de 64 bits.

Y pagar 270.000 pts (más de 1.600 euros) por ella. Por 10.000 ptas. más (60 euros) se podría tener el sistema con DVD. Y por unas 20.000 ptas. más (120 euros) un procesador a 400 Mhz. Una grabadora de CD de doble velocidad lo encarecía en 50.000 ptas. (300 euros). Si se quería equipar al sistema con una unidad ZIP externa de 2 gigas, podía costar 85.000 pts. (500 euros).

También se podían comprar sistemas de gama baja, con procesadores Celeron con 32 megas de RAM, disco duro de 2 gigabytes y monitor de 14 pulgadas por 130.000 ptas.

(unos 800 euros). Esta misma configuración en un portátil, rozaba las 300.000 ptas. (1.800 euros) y podía pesar más de 3 kilos. Aun con estos precios, en el primer trimestre de 1998 se bate un récord y se veden 233.000 ordenadores. Una configuración parecida pero con conexión Ultra/Wide SCSI y de marca DELL podía salir por 500.000 pts (3.000 euros).



_ En octubre American Airlines se convierte en la primera línea aérea en ofrecer **billetes electrónicos** en 44 países a través de su página aa.com. Rápidamente el sistema es adoptado y hoy la mayoría de los billetes han dejado de ser físicos.

_ **Pokemon** llega a Estados Unidos. Tardaría varios años más en llegar a España y convertirse en un fenómeno en videojuegos, televisión y todo tipo de productos de márketing. 160 millones de juegos vendidos hasta la fecha avalan el éxito comercial de una imagen reconocida en todo el mundo con sólo 12 años de vida (fue creado en 1996).



_ En febrero de 1998, **XML 1.0** se convierte en una recomendación de la W3C. Su diseño comenzó dos años antes. XML se convertiría desde entonces en un estándar ampliamente aceptado y de gran éxito entre programadores. XML tiene sus raíces en un lenguaje de IBM de los setenta, llamado GML (Generalized Markup Language), que surgió de la necesidad de IBM de almacenar grandes cantidades de información. En 1986 ISO comenzó a trabajar para normalizarlo, creando SGML, que sentaría las bases de XML. A principios de 1998, sólo un 1% de páginas usan XML. Para cuando acabase el año ya serían un 16%.

_ En 1997 Network General y McAfee Associates se funden en **Network Associates**, que a su vez en 1998 compran (por 640 millones de dólares) Dr. Solomon's. Dr.Solomon's Antivirus Toolkit era líder europeo en Antivirus y se podía comprar por 37.000 pts (220 euros). Más tarde todo quedaría bajo la marca McAfee.

_ Para conectarse a Internet, un modem de 33600 bps. puede costar 10.000 pts (60 euros). Una cámara digital Casio de 1.3 megapixeles, con 8 megas, **capaz de grabar películas de hasta 6.4 segundos**, cuesta 109.000 pts. (más de 600 euros).

_ Nace **Red2000** un canal temático de informática en Vía Digital (que en 2003 se fusionaría con su principal rival Digital+). Se une así al canal C: que comenzó a emitir en 1997.

_ **Nicholas Negroponte**, gurú tecnológico, vaticina que: "En cinco años [a partir de 1998, se entiende] la gente delegará en agentes la tarea de navegar por Internet. Pero el comercio electrónico moverá billones de dólares y los sistemas de pago se diversificarán, creándose nuevas monedas basadas en bits. Todas las cosas que nos rodean tendrán una dirección IP, con lo que se generará información propia que servirá para que la intervención de los intermediarios desaparezca". Definió el correo basura como el enemigo número uno del comercio electrónico.

_ Augusto Pinochet es detenido en Londres por orden de **Baltasar Garzón**.

_ El último minuto de 1998 dura 61 segundos. Se introduce un **"leap second"** o **"segundo bisiesto"** que alarga el día en un segundo. Es un ajuste parecido al que se realiza con los años bisiestos, pero que sólo añade un segundo para compensar las pequeñas diferencias entre el ritmo de la rotación de la Tierra con la escala de tiempo UTC (Coordinated Universal Time). La Tierra gira a un ritmo que decrece continuamente, con una desaceleración pequeña y conocida. Por el contrario, el tiempo es medido a través de relojes atómicos muy precisos que son estables. Se desfasan cada cierto tiempo y hay que corregirlos para que

la hora “solar” y la hora medida por los humanos sigan parejas. Existe la alternativa de dejar pasar esos segundos y añadir un día extra cada varios siglos, pero desde 1972 se viene haciendo regularmente (casi todos los años de la década de los 70) y cada varios años actualmente. Al último día de de 2005 y de 2008 también se le añadirá un segundo.

_ En la una-al-día de 23 de noviembre, **“Incompatibilidad entre K6-2 de AMD y Windows 95”** se incluye por primera vez la cabecera en cada correo enviado:

HISPASEC una al día (23/11/98)
Todos los días una noticia de seguridad
----

en junio de 2000 se cambiaría a la actual que se mantendría hasta hoy.

Hispasec - una-al-día 18/06/2000
Todos los días una noticia de seguridad www.hispasec.com

Seguridad Informática

En junio, lo que Microsoft llamaba internamente Proyecto Memphis se convierte en **Windows 98**, uno de los sistemas operativos más esperados tras el bombazo de Windows 95 (englobado en el proyecto Chicago pero sin todo lo que se esperaba de él. “Chicago” todavía se puede ver en los archivos de configuración de los sistemas actuales). Windows 98 no supone una ruptura total con lo que venía siendo el sistema operativo de la compañía (MS-DOS 6.2, su última edición) pero sí que resulta en una interesante revisión de Windows 95.

En abril, en el Comdex se produce una anécdota muy sonada. Bill Gates presenta su sistema operativo Windows 98 y sus virtudes. En el momento de de hablar de su funcionalidad Plug and Play (PnP), Chris Capossela enchufa un escáner en el ordenador para comprobar cómo lo reconoce. El sistema se paraliza al intentar instalar el dispositivo y muestra la BSOD (pantallazo azul de la muerte). Tras los vítores, risas y aplausos del público, Gates dice “That must be why we’re not shipping Windows 98 yet.” El vídeo está disponible en YouTube.

Las diferencias en cuestión de seguridad con Windows 95 son nulas: los dos carecen casi por completo de funcionalidades de seguridad. La fama negra de Microsoft se agranda a pasos agigantados y le perseguiría a pesar de sus esfuerzos. Su éxito sería tal que Microsoft mantendría el soporte del sistema operativo hasta el 11 de julio de 2006.

_ Sin duda, es el año de **“Estados Unidos contra Microsoft”**. La compañía es acusada ante los tribunales, alegando que Microsoft está abusando de su poder monopolístico para vender su navegador

junto con su sistema operativo Windows 98. Microsoft incrustó de forma inseparable su Internet Explorer con su Windows 98, y esto es tachado de juego sucio por parte de toda la comunidad. Para obtener Internet Explorer con su anterior sistema operativo, había que instalarlo como una aplicación más, pero en Windows 98 viene de serie y no hay forma oficial de eliminarlo. Es el momento en el que el navegador Netscape está en su mayor apogeo y Microsoft quiere su parte de la tarta de los navegadores. Es el año en el que Internet Explorer gana más adeptos, pero sin duda influye el hecho de que todo usuario de Windows dispone ahora de forma gratuita del navegador, a mano y por defecto, con lo que el resto quedan en desventaja. Incluso se acusa a Microsoft de alterar las APIs para favorecer a su navegador sobre otros. Para Microsoft, la incrustación del navegador es el resultado de un mejor rendimiento y compatibilidad entre navegador y sistema operativo, que suponía una ventaja para sus clientes. Sus detractores alegan: ¿Si IE está disponible para Mac de forma independiente, por qué no para Windows?



_ Chen Ing Hau crea el **virus CIH o Chernobyl** (que lleva sus propias iniciales). Justificaría su creación por una venganza en contra de los que llamó "incompetentes desarrolladores de software antivirus". Denomina a su criatura Chernobyl en conmemoración del día del aniversario de la catástrofe ocurrida en la planta nuclear soviética. Sería calificado como uno de los virus más poderosos, por atacar al hardware del sistema. Modificaba o destruía la programación de la BIOS, sobreescribiendo parte de este firmware. Tendría diferentes variantes.



_ **Linus Torvalds** obtiene la marca legal de "Linux". Se lanza la versión del kernel 2.2, aunque la verdaderamente estable se considera todavía la rama 2.0. Aparecen versiones avanzadas de sistemas operativos que usan el kernel Linux como Red Hat 5.1, Slackware 3.5 y OpenLinux 1.1 de Caldera.

_ El 7 de septiembre dos jóvenes universitarios que pretendían terminar su postgrado en la Universidad de Stanford constituyen una pequeña firma llamada **"Google Inc."**. Larry Page y Sergey Brin cubren así legalmente un buscador de enlaces web que habían creado un par de años antes con el nombre de BackRub. Posteriormente sería bautizado como Google en honor al término "googol". Es un término acuñado en 1938 por Milton Sirotta (de 10 años) sobrino del matemático estadounidense Edward Kasner para dar nombre a 10 elevado a 100. Sientan las bases de lo que se convertiría en una de las marcas más reconocidas del planeta. Mientras, el usuario tecleaba Excite, Infoseek, Inktomi, AltaVista o Yahoo! para realizar sus búsquedas. Nace Biwe, un buscador español que pasó sin pena ni gloria.



_ Tras la Sega Saturn, aparece en Japón la **Sega Dreamcast**, una consola adelantada a su tiempo que fracasaría. Llegaría a Europa en 1999. Cuesta unos 200 dólares del momento. Tiene 16 megas de RAM, 8 de vídeo, 200 Mhz de procesador y 2 megas de RAM para sonido. Por primera vez, posee un módem incorporado y soporta el juego en línea. Sony todavía pelea con la Playstation 1 y Nintendo con su Nintendo 64.

_ En septiembre se crea la **Internet Corporation for Assigned Names and Numbers** (más conocida como ICANN). Establecida en California, ICANN es una compañía sin ánimo de lucro creada para ordenar ciertas tareas en Internet de las que antes se ocupaba IANA (Internet Assigned Numbers Authority) en nombre del gobierno de los Estados Unidos. ICANN controla el reparto de direcciones IP y el manejo de dominios primarios. En 2003 jugaría un papel determinante a la hora de "convencer" a Verisign para que retirase su controvertido servicio de DNS "Site Finder".

_ AOL compra Netscape y Netscape funda la **Mozilla Organization**. En principio su función era coordinar el desarrollo de la Mozilla Application Suite (actualmente Seamonkey Suite). Aunque estaba compuesto básicamente de trabajadores de Netscape, operaba independientemente. El navegador Mozilla en aquel momento no estaba pensado para ser usado por usuarios finales.

_ Ericsson, IBM, Intel, Nokia y Toshiba comienzan a desarrollar las especificaciones de una nueva tecnología de transmisión bajo el nombre en código de **Bluetooth**.

_ Se lanza con gran éxito el juego **Commandos** para PC. Tecnología nacional que devuelve a España su éxito en la creación de videojuegos, olvidada con el Spectrum.

_ La versión de **Norton Anvirus Deluxe 4.0**, incluye un método para "actualizar el antivirus de forma gratutita a través de Internet, con sólo pulsar un botón", cosa que es "conveniente hacer de vez en cuando".

_ Se cree que el **DHTML** podría oscurecer el futuro de Flash en Internet.

_ **Apache lanza su versión 1.3**, que aporta numerosas mejoras en el rendimiento del sistema. Para mediados de año, copa justo la mitad de los sistemas web de Internet. La rama todavía sigue estando operativa, debido a que marcaría un antes y un después en el desarrollo del servidor web. La versión de Internet Information Server 4.0, aparecida con Windows NT 4.0 en su Option Pack a finales de 1997, ya es muy usada durante el año, aunque su versión 3.0 todavía tiene bastante éxito. Para ese año el servidor de Microsoft copa el 20% de uso de servidores web. IIS 4.0 se convertiría en un verdadero quebradero de cabeza para la seguridad en Microsoft. Se resarciría años después con excelentes resultados en seguridad en su versión 6.0 y 7.0.

_ Aparece en octubre el **Service Pack 4 para Windows NT 4.0**. Sus problemas e incompatibilidades serían objeto de la primera una-al-día publicada por en octubre de 1998.

Internet no se entiende sin **Netscape**, el navegador que usa la mayoría... pero ese año cambiaría todo. Internet Explorer aparece por primera vez en el paquete opcional Plus! para Windows 95, y no arrasaría con todo hasta 1999. En aquel momento su versión 4.0, aparecida en septiembre de 1997, es la más usada. En 1998 gana rápidamente adeptos "gracias" a la maniobra de la compañía de incluirlo de serie en Windows 98. Durante todo el año se libra una dura batalla de navegadores, donde la balanza cambia radical y rápidamente en favor de Microsoft. Empieza el año con un 40% de usuarios, frente el casi 60% de Netscape, y termina 1998 ganando con la mitad de la tarta y dejando un 47% para su principal competidor, que nunca más se recuperaría.

Opera es todavía minoritario, va por su versión 3. Ese mismo año la compañía decide apostar por desarrollar un navegador especialmente diseñado para los dispositivos móviles. A la postre resultaría un acierto para la empresa.

_ Hay ya **100 millones de usuarios** de Internet en el mundo. En España, poco más de un millón. 7,5 millones de usuarios tienen ordenador.

_ Se lanza el procesador **K6-2**, competencia directa de los **Pentium**. Una de las diferencias con respecto

al Pentium al que planta cara, es que sigue fiel a la conexión Socket 7, mientras que Intel apostó para sus Pentium 2 por el Slot 1 (en perpendicular a la placa).

_ Las **Palm Pilot** son los PDA más vendidos. Su nombre quedaría prácticamente como sinónimo de PDA.

_ Apple, después de unos años de crisis sin productos novedosos, comienza su resurgimiento y lanza los **iMac** con un estilo futurista y moderno. Llamados "Bondi Blue", tienen un procesador G3 y una carcasa translúcida que luego se comercializaría en distintos colores. Comienza la rama iMac que perdura hasta hoy. Este primer iMac se dejaría de fabricar en 2003. Usó el sistema operativo Mac OS 8, Mac OS 9, Mac OS X y pasó de los 233 a los 700 Mhz. Comenzó con 4 gigas de disco duro.

_ **StarOffice 4.0** se lanza para competir contra Office 97.

_ Se lanza **Qmail**. El servidor de correo de código abierto destinado a la seguridad. Se ofrecen 1.000 dólares a quien encontrase una vulnerabilidad grave en él. Nadie lo ha conseguido todavía, diez años después.

_ Se venden kits de acceso a Internet como, por ejemplo, el de **Teleline**: Un año de acceso a Internet más móden 33.600 bps. Por 20.000 pts. (120 euros). Jet Internet ofrece también un año de acceso a través de RDSI, con tarjeta por 45.000 pts. (270 euros).

_ Nace **Info Vía Plus** para sustituir a infovía.

_ El 12 de marzo de 1998 se publica el **primer número de Ciberp@ís**, en forma de pequeño periódico dedicado a Internet. Una publicación de calidad que apostó desde el primer momento por la información útil sobre la red.

_ **Juan Carlos García Cuartango** se convierte en la pesadilla de Microsoft. El ingeniero español comienza a estudiar el navegador Interntet Explorer en busca de problemas de seguridad en 1998 y descubre lo que se llamó el "agujero Cuartango" en él. El agujero permitía ejecución de código a través de JavaScript (diez años después sigue siendo el origen de la mayoría de los problemas de seguridad de los navegadores actuales). Después viene la "ventana de Cuartango"... y desde entonces pasaría años desvelando vulnerabilidades cada poco tiempo, ayudando así a mejorar la seguridad del navegador. Junto con Georgi Guninski, desvelaron la mayoría de los problemas de seguridad en Microsoft a finales de los 90.

_ La adquisición de **PGP** por parte de NAi levanta discusiones en todos los círculos de la criptografía acerca del camino que seguirá este programa. www.pgp.com redirige a la web de Network Associates. Asegura que seguirá distribuyendo este programa en las mismas condiciones que se ha venido haciendo hasta ahora: gratuito y ofreciendo las fuentes de esta versión al público general. Zimmerman abandonaría el proyecto pocos años después.

_ **El 28 de diciembre nace Hispasec** como un portal de noticias con presencia web. Desde octubre, se habían publicado a través del boletín de correo suficientes boletines como para recopilarlos y publicarlos en una página. Además, así cualquiera podía suscribirse a una-al-día. Bernardo Quintero utiliza el dominio www.hispasec.com para este fin. La página se monta sobre un "viejo" PC que él mismo tiene en casa, con procesador Cyrix. Se hospeda de forma "gratuita" en el CPD de un ISP de Málaga para el que Bernardo había comenzado a trabajar por las tardes, administrando y asegurando los sistemas.

Una al día

01/11/1998 WinScript.Rabbit, una nueva generación de virus dirigidos a Internet.

Se presenta dentro de la nueva ola de virus dirigidos a Internet, WinScript.Rabbit es capaz de infectar ficheros script de Windows sobreescribiéndolos con sí mismo. Lo más peligroso de este virus es que es capaz de propagarse a través de Internet, ya que las últimas versiones de los navegadores ejecutan los ficheros scripts de forma local aunque se encuentren alojados en servidores remotos.

La idea de este virus es muy antigua, tenemos que remontarnos a los orígenes de los virus en los sistemas UNIX. En los años 80 los virus escritos en lenguajes scripts clónicos para UNIX se convirtieron en autenticas plagas para las redes de ordenadores de por aquel entonces. Conocidos como “gusanos” son de destacar el “Christmas Tree,” HI.COM y “Wank Worm”. Ahora WinScript.Rabbit se presenta como la nueva generación de “gusanos” en la era Windows/Internet.

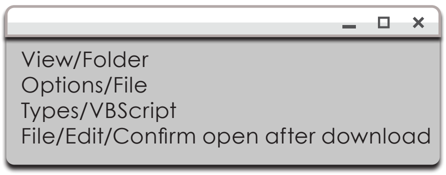
Es el primer virus identificado que afecta a los ficheros scripts de Windows. Su código es xtremadamente simple, apenas contiene 10 comandos, y todo parece indicar que su origen proviene del grupo “CodeBreakers”. El virus contiene algunos fallos que provocan que se detecte fácilmente cuando infecta un sistema. Cuando un navegador lo ejecuta el virus infecta todos los ficheros de la caché del navegador, y los copia al escritorio de Windows, que es el directorio por defecto de los navegadores. Cuando esto ocurre, el escritorio se inunda de iconos correspondiente a los ficheros infectados. El nombre de Rabbit proviene de su facilidad para la reproducción similar a la de los conejos.

Pese a los graves fallos de funcionamiento y su simplicidad, este virus representa una amenaza potencial para todos los usuarios de Internet, ya que puede servir de base para virus más sofisticados que utilicen el mismo principio de propagación. Es probable que en el fúturo surgan nuevos virus que aprovechando las características de los navegadores y de los sistemas Windows infecten otros tipos de ficheros además de los scripts.

El virus trabaja bajo todas las versiones de Windows 32bits (Windows 95/98/NT) si se encuentra instalado el Microsoft Scripting Host, el cual viene por defecto activado en las versiones 98 y NT 5.0 (Windows 2000). En el resto de sistemas windows puede encontrarse si se han actualizado determinados componentes.

Para protegerse de este nuevo tipo de virus debemos de activar la siguiente protección:

Internet Explorer Windows 98:



En Netscape no existe una opción para la ejecución de ficheros scripts. Por el momento no se ha detectado propagación de este virus en Netscape.

Bernardo Quintero

03/11/1998 El Gusano de Morris, 10 años despues.

El 3 de noviembre de 1988, tal día como hoy, miles de ordenadores sucumbieron ante el engendro de Robert Tappan Morris, un estudiante de 23 años de la Universidad de Cornnel Al llegar a sus puestos de trabajo, los administradores no daban crédito al ver como sus VAXs y SUNs se bloqueaban en cadena, víctimas de una sobrecarga de tareas invisibles. Ninguno era consciente de que estaba siendo testigo de excepción de lo que ha llegado a ser un mito en la informática y las comunicaciones, aquellas 99 líneas de código, causas del desastre, han dado lugar a lo que hoy se conoce como: el Gusano de Morris.

No son pocas las discusiones que siempre se han mantenido sobre si el término "gusano" es o no apropiado para describirlo, o si por el contrario deberíamos hablar del primer "virus" de red. La principal diferencia entre un "gusano" y un "virus" tradicional la podemos encontrar en el método de operar a la hora de reproducirse. Cuando un "virus" estándar entra en un ordenador el suele alterar un fichero al que se adjunta. Cualquier uso posterior del fichero infectado hará que éste se active, siempre de forma transparente al usuario. El "virus" se encontrará en el sistema sin dar señales de vida aparentes, hasta que ejecute su efecto (payload) en una fecha determinada ó por otra condición que el programador del "virus" haya elegido. Además, para lograr pasar de un ordenador a otro necesita que un fichero infectado sea traspasado por la acción de un usuario.

En el otro lado, cuando un "gusano" entra en un ordenador, normalmente a través de Internet, comienza una busqueda de otros sistemas conectados a la Red que puedan ser victimas de su infección. Al contrario que los "virus", no existe un estado de latencia, el se activa nada más infectar el ordenador, y no necesita adjuntarse a ningún fichero. Para lograr su cometido se basa en los "agujeros" de otros sistemas que le permita introducirse en ellos, y continuar su infección. Es una especie de "virus hacker" que explota los fallos de seguridad de los sistemas para reproducirse. En el caso del Gusano de Morris, explotaba vulnerabilidades bien conocidas del s.o. Unix. Por ejemplo, la versión del sendmail de aquella época permitía conocer los usuarios de forma remota. Simplemente probando cuentas cuyos nombres de usuarios y passwords coincidieran, el Gusano consiguió gran cantidad de accesos.

El origen de los "gusanos" deriva de los años 60, cuando en los laboratorios AT&T Bell se originó el juego "Core Wars" ó guerra de núcleos de ferrita. La memoria de nucleo de ferrita contenia tanto conjunto de instrucciones como de datos. El juego consistía en crear un programa que al reproducirse fuera ocupando toda la memoria, al tiempo que borraba de ella al programa del contrincante. El jugador cuyo programa conseguía hacerse con toda la memoria, o que tras transcurrido un tiempo tenía mayor número de reproducciones, ganaba la partida.

Parece clara la relación entre estos juegos de los años 60 y el Gusano de Morris. Sin embargo, un estudio más detallado nos llevará a comprender hasta que punto se estrechan los lazos entre estas historias. Los tres estudiantes que dieron origen, en los laboratorios AT&T Bell, a "Core Wars" respondían a los nombres de H.Douglas McIlroy, Victor Vysottsky y Robert Morris. No, no se trata de una equivocación, Robert Morris de los laboratorios AT&T de los años 60 es, ni mas ni menos, que el padre de Robert Morris creador del Gusano.

Pero aun hay más, un estudio detallado del código del Gusano de Morris viene a demostrar la existencia de dos programadores. Todo parece indicar que Robert Morris hijo utilizó parte de los programas creados por el padre en "Core Wars", junto con documentación reservada de los laboratorios Bell, donde su padre fue uno de los desarrolladores del UNIX. Al fin y al cabo, de tal palo, tal astilla.

Bernardo Quintero

07/11/1998 DeepThoat se suma a la moda de los troyanos.

Tras los ya conocidos BackOriffice y NetBus aparece un nuevo troyano con características de administración remota, DeepThroat. Al igual que con BO y NetBus la herramienta se compone de dos partes claramente diferenciadas, el cliente y el servidor. El cliente que aparce bajo el nombre de RemoteControl, se usa para controlar los ordenadores afectados mientras que el programa Systempatch es el servidor. DeepThroat (http://hax0r.to/deept/) es una herramienta de administración remota para 95/98. Básicamente es una herramienta freeware con capacidades similares a las que ya disponían NetBus y BO.

El cliente permite acceso a la unidad de CD, abriendo y cerrando la unidad de forma remota, también permite el envío de cajas de mensjaes, ocultar y mostrar la barra de inicio. Al instalar el servidor también se procede a la instalación de un servidor de ftp a través del puerto 21, gracias al que se puede subir y bajar ficheros del ordenador afectado sin ningún problema. Se puede ver la pantalla del ordenador infectado gracias a la posibilidad de efectuar una captura de pantalla, en formato jpg y de unos 80kb que será enviada de forma automática al cliente. No permite ver la pantalla del ordenador remoto en tiempo real, pero si puede dar una buena idea de que hay "en el otro lado".

Algo que puede llegar a resultar muy molesto es la posibilidad de encender y apagar el monitor remoto. Esta función hace que el monitor pase al estado de ahorro de energía y sólo puede ser restaurada de nuevo de forma remota. Igual de molesta puede resultar la opción de rebotar el ordenador.

Por último DeepThroat incluye un scanner que permite buscar ordenadores con el servidor instalado. El equipo de I+D de HispaSec investigará y comprobará más a fondo el funcionamiento de DeepThoat esperando seguir informandoos sobre esta nueva herramienta.

Bernardo Quintero

08/11/1998 Virus infector de html

Ha nacido una nueva generación de virus, HTML.Internal es el primer virus conocido capaz de infectar archivos html. HTML.Internal busca ficheros html en los discos infectándolos. Para difundirse a sí mismo el virus usa rutinas de script escritas en Visual Basic que incluye dentro del código html. El virus sólo es capaz de replicarse en caso de que los niveles de seguridad del navegador permitan la ejecución de rutinas de script con capacidad de acceder a los archivos del disco. Por defecto ésta opción viene desactivada y al acceder a un archivo infectado se muestra un mensjae de error.

La cabecera de los archivos html infectados contienen la referencia a un script (rutina principal del virus) que es ejecutada automáticamente cuando el navegador accede al archivo infectado. Cuando la rutina principal del virus toma el control está llama a la rutina de infección con una probabilidad de 1/6 dependiendo de un contador aleatorio, en caso contrario se devuelve el control.

Usando instrucciones Visual Basic el virus busca todos los archivos *.htm y *.html en el directorio actual y superior infectándolos. Cuando el el virus infecta un archivo se escribe asimismo al comienzo del fichero sin ningún daño para los datos de los ficheros.

La cabecera del virus contiene la siguiente línea que lo identifica:

<html> <!--1nternal-->
Después de infectar el virus muestra «HTML.Prepend /1nternal» en la barra de estado de Windows.

Antonio Ropero

03/12/1998 USA nos exporta sus restricciones criptográficas.

Los Estados Unidos y la administración Clinton no contentos con imponer su severa política de exportación de material criptográfico han convencido a otras 33 naciones, entre las que se incluye España, para que sigan sus directrices en esta materia.

En una reunión celebrada ayer jueves tres de diciembre, las 33 naciones que firmaron el acuerdo de Wassenaar (www.wassenaar.org) limitando la exportación de armamento se mostraron de acuerdo en imponer controles a las tecnologías más avanzadas de encriptación de datos, incluyendo el software destinado al mercado de masas. Entre las naciones firmantes de este acuerdo se encuentran potencias como Japón, Alemania y Gran Bretaña.

De esta forma Estados Unidos ha conseguido convencer a otras naciones de que sigan sus mismas directrices en la materia de exportación de software de encriptación de datos.

Compañías de alta tecnología estadounidenses, como Microsoft e Intel, se habían quejado de que la carencia de restricciones en otros países obstaculizaba su capacidad de competir al exterior. La industria pedía que las restricciones americanas se relajaran o eliminaran totalmente, pero no ha pedía controles más apretados en otros países.

Los abogados de la privacidad también se han opuesto firmemente a los controles de la exportación en el cifrado de los EE.UU., discutiendo que las tecnologías de encriptación proporcionarán los medios cruciales para proteger la privacidad en la era digital.

La nueva política excluye específicamente del control a aquellos productos, como películas o grabaciones enviadas a través de Internet, que usen la encriptación para proteger la propiedad intelectual del copiado ilegal.

Según las claves del acuerdo firmado, los países miembros del tratado restringirán las exportaciones de productos de encriptación general que usen claves superiores a 56 bits, los productos destinados al mercado de masas tendrán una limitación de 64 bits.

Ahora será cada uno de los países los que deban redactar sus propias leyes para la implementación del acuerdo. Las 33 naciones firmantes de este restrictivo acuerdo son las siguientes: Argentina, Australia, Austria, Bélgica, Bulgaria, Canadá, República Checa, Dinamarca, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Japón, Luxemburgo, Holanda, Nueva Zelanda, Noruega, Polonia, Portugal, República de Corea, Rumanía, Rusia, República Eslovaca, España, Suecia, Suiza, Turquía, Ucrania, Reino Unido y Estados Unidos.

En estos momentos en HispaSec mostramos una gran preocupación por lo que pueda representar este tratado, esperando que no afecte a la libertad y la privacidad de todo el mundo. ¿Cuál es el futuro del PGP? ¿Qué pasará con la versión internacional de PGP? ¿Cuál es la opinión de las compañías que se puedan ver afectadas por la restricción? Todo parece indicar que cada día nos quieren dificultar más la libertad y poner más trabas a la privacidad.

Antonio Ropero

13/12/1998 El sistema militar británico indefenso ante el 2000.

Según el último informe elaborado por la secretaría de defensa Británica, se detectan graves problemas en todos sus sistemas informáticos para la transición al año 2000. Un 90% de los sistemas informáticos más importantes de la marina de su Majestad no están preparados para el cambio de milenio. Este problema no sólo afecta a la armada, ya que también se ven afectados el 65% de los sistemas de las Fuerzas Aéreas, el 82% de los Sistemas de la Secretaría de Defensa y el 50% de los sistemas del Ejercito de Tierra.

Los ordenadores que controlan los misiles Trident, también se ven afectados, lo que hace ha este problema tomar un cariz más peligroso, ya que estos misiles portan cabezas nucleares.

La falta de tiempo para poder realizar una óptima comprobación, añade una mayor peligrosidad al tema, ya que la previsión realizada por la Secretaría de Estado, estimaba que la optimización debería haber finalizado para el 31 de Diciembre de 1.998. Esto hubiera dado un margen de un año para la comprobación de todos los sistemas informáticos. Las autoridades británicas consideran tras dos años de actualización, imposible de cumplir los plazos preestablecidos.

Antonio Ropero

14/12/1998 Una nueva generación de virus informáticos ha llegado.

El intercambio de disquetes y aplicaciones ha sido la vía principal de transmisión de virus informáticos. Con la llegada de Internet llegan también los nuevos virus capaces de viajar por la red para infectar maquinas situadas a miles de kilómetros. La primera muestra de esta nueva amenaza nos llega una vez más de la mano de 29A. Para los menos introducidos en éste mundo, 29A es un grupo español de programadores dedicados a la investigación y desarrollo de vida artificial, especialmente de virus informáticos.

Win32.Parvo es un virus capaz de infectar ordenadores remotos, utilizando técnicas de propagación por red. Esto significa que el virus es capaz de transmitirse desde una maquina infectada a otra mientras la primera está conectada a Internet.

En un primer análisis descubrimos que Win32.Parvo es un virus altamente polimorfo, que infecta aplicaciones tanto de Windows95 y 98 como de WindowsNT. Los programas infectados se ejecutan sin ningún problema, y el usuario puede permanecer infectado durante meses antes de descubrir que su maquina ha sido invadida.

Tras realizar varias pruebas descubrimos que Win32.Parvo infecta varias aplicaciones destinadas a Internet, especialmente el navegador y el cliente de correo. Cuando se utilizan estos programas es porque, normalmente, estamos conectados a Internet, momento que aprovechará el virus para crear una imagen virtual de si mismo en el mismo formato que los clientes de correo utilizan para mandar attachments. Sin la intervención del usuario y sin delatar su actividad, el virus se envía a si mismo por mail. Tras este descubrimiento a todos nos surge la misma duda: ¿y a quien se envía? ¿de donde obtiene el virus las direcciones de mail de otros usuarios?

Después de trastear un poco mas dentro del código vírico nos encontramos con la respuesta. El virus se conecta a un grupo de news elegido al azar y extrae de él un mensaje cualquiera. Seguidamente busca la dirección de correo del remitente y esa será su próxima víctima.

Cuando otro usuario recibe un correo infectado, nada hace sospechar que se trata de un virus. El virus

es capaz de generar distintos tipos de mensajes, hablando de distintos temas y con direcciones de origen «spoofed» (falseadas) en las que el remitente parece ser unas veces Microsoft u otras empresas. Los mensajes tienen algo en común, todos llevan un fichero adjunto en el que reside el virus, y que infectará el navegador y el cliente de correo si el usuario lo ejecuta, con lo que el ciclo de vida se completa.

Win32.Parvo presenta cualidades que le aproximan a lo que conocemos como «worms» (gusanos) puesto que no necesita infectar los programas para llegar a otras maquinas. No obstante el virus se establece dentro de varias aplicaciones de Windows para asegurar así su permanencia en el sistema.

Este virus es el pionero en este tipo de transmisión, pero sospechamos que no es mas que el comienzo de lo que será una larga lista de virus de nueva generación.

Antonio Ropero

21/12/1998 Nuevo Virus que ataca a través de redes locales.

En los últimos días nuevos virus han visto la luz, Itaqua, Parvo o el primer virus para PowerPoint se han pasado por esta sección de noticias en pocos días. En esta ocasión un nuevo virus salta a la luz por haber tenido en jaque durante todo el fin de semana al gigante de las comunicaciones MCI WorldCom. Network Associates (http://www.nai.com), el fabricante del antivirus McAfee, ha designado este ataque como un caso de «ciberterrorismo», pero MCI WorldCom (http://www.mciworldcom.com/) afirma que sus operaciones no se vieron afectadas. Aunque según comentarios internos a los que HispaSec ha tenido acceso «el sistema informático de MCI se ha derrumbado y ha afectado a varios lugares por culpa de un virus informático, lo que ha traído de cabeza durante el fin de semana a media empresa».

El portavoz de MCI ha rechazado informar acerca de la propagación del virus en su red, o de cuantos ordenadores se vieron afectados por «Remote Explorer», (Explorador Remoto) nombre asignado a este nuevo virus. El virus que parece que se propaga a si mismo sobre redes Windows NT, ha sido identificado hoy lunes por Network Associates que ha colaborado con MCI para contener el virus desde que éste fuera detectado el pasado jueves.

La misma Microsoft ha confirmado que también ha trabajado desde sábado con Network Associates para combatir el virus. Según la empresa de Bill Gates el virus se propaga sobre ordenadores con Windows NT bajo plataforma Intel pero solamente cuando funcionan en modo «administrador».

Remote Explorer comprime archivos de programa de tal forma que no pueden ejecutarse, y encripta ficheros de datos por lo que los usuarios no pueden tener acceso a ellos. Microsoft ha afirmado que la solución al problema recupera los datos perdidos y devuelve las máquinas a su configuración original.

El virus es residente en memoria e infecta ficheros exe, txt y html, tanto en NT Server como NT Workstation, propagándose rápidamente a través de entornos de red. La característica principal y más destacada de Remote Explorer es su capacidad para transmitirse y replicarse a si mismo a través de la red sin la intervención típica del usuario, lo cual le otorga cualidades propias de los «gusanos».

La detección del virus en un sistema resulta fácil de comprobar. Basta con acudir al «Panel de Control» de Windows NT y listar los «Servicios» que se están ejecutando, si se encuentra uno nombrado como «Remote Explorer» evidenciará la presencia del virus. Otra forma de detectar el virus es a través del «Administrador de tareas». Si entre los «procesos» listados se encuentran «ie403r.sys» o «taskmgr.sys» (no .exe) el sistema estará infectado.

Sorprendentemente se trata de un virus con un gran tamaño. Sus 125 Kbytes lo convierten en todo un gigante, especialmente comparándolo con los tamaños habituales de 10 Kbytes aproximadamente del otros virus. Este tamaño, puede venir dado al estar escrito en C, contando con unas 50.000 líneas de código y estimándose en 200 horas las labores de programación del virus.

El virus lleva una dll consigo para el proceso de infección, pero si la dll se borra el mismo creará otra copia. El virus incluye una rutina de tiempo, diseñada para aumentar su velocidad en el proceso de infección y búsqueda durante el periodo que comprende las 3:00 PM de cualquier sábado hasta las 6:00 AM del siguiente domingo. Otra característica sorprendente del virus es su ausencia de payload, o acción que lleva a cabo en su activación.

Si se localiza un sistema infectado en el entorno de red, es recomendable aislar dicho ordenador y determinar que maquinas están en conexión directa con ella, desactivando, de igual forma, la conexión a la red de estas otras. Como el virus infecta la memoria es necesario arrancar con un disquete limpio para proceder a su detección y limpieza. Network Assiciates dispone de un detector gratuito para Remote Explorer en sus páginas web, en la dirección http://www.nai.com/products/antivirus/remote_explorer.asp

Antonio Ropero

31/12/1998 Adiós 1998, Feliz 1999.

Se acaba el 1998, y damos la bienvenida a un nuevo año. Un 1998, que ha significado el nacimiento de HispaSec y que ha estado lleno de noticias. Vamos a aprovechar este último día del año para realizar un breve repaso a las noticias publicadas más destacadas.

La andadura de una-al-día nació un 28 de octubre y fue exactamente dos meses después, el 28 de diciembre cuando se abría al público nuestro web (www.hispasec.com). Nuestra primera noticia hacía referencia al Service Pack 4 y todos los problemas que se habían encontrado en él.

El tema vírico junto con el de Internet ha sido las materias que más artículos han generado en nuestro servicio de noticias. Hemos cubierto el nacimiento de nuevas tecnologías víricas, como los virus de script, los troyanos de Internet, con un estudio especial sobre el DeepThroat, los virus html o el primer virus para PowerPoint. También hemos dedicado un espacio a virus españoles como el Win32.Parvo o el Ithaqua. Internet y las vulnerabilidades encontradas en determinados sistemas ha generado importantes noticias. Los fallos descubiertos por el español Juan Carlos García Cuartango han sido noticia en múltiples ocasiones, otros sistemas vulnerables de los que nos hemos hecho noticia han sido el SHH, BIND, routers cisco, el KDE, MS-Proxy, etc.

Pero también hemos informado de hechos importantes y relevantes en el mundo de la seguridad informática. La propuesta del PGP como estándar, el tratado de Wassenar, la problemática de Internet en China, o la reducción de las medidas en la limitación de exportación de material criptográfico por el gobierno estadounidense.

El 2000 y toda la problemática asociada también ha venido a ocupar una parte importante de este servicio de noticias. Sin duda el próximo año 1999, el problemático año dará mucho más que hablar. Para acabar sólo nos queda desear un feliz año nuevo a todos nuestros suscriptores.

Antonio Ropero


Juan C. G. Cuartango

Juan Carlos García Cuartango salta a la fama en 1998 cuando (con 38 años) de forma obstinada y continua, comienza a encontrar problemas de seguridad en el inmaduro Internet Explorer. El agujero de Cuartango, la ventana de Cuartango... junto con Guninsky, protagoniza una época en la que los investigadores privados demuestran las carencias de un software muy popular, poniendo en evidencia a los desarrolladores y, a la vez, motivándolos para mejorar la seguridad del producto. Una-al-día se alimentó durante mucho tiempo de sus descubrimientos, desde donde se le daba la repercusión mediática necesaria.

Hispasec: ¿Con qué edad empezaste a tener contacto con la informática? ¿Recuerdas los primeros equipos informáticos que pudiste trastear?

Juan Carlos García Cuartango: Antes de la informática estaba la electrónica. Recuerdo una radio con un diodo de germanio, un condensador y una bobina construida sobre el cartón de un rollo de papel higiénico enchufada al radiador y al somier de la cama. Esto marcó mi futuro hacia las telecomunicaciones cuando yo tenía 12 años. Después ya en la veintena conocí el ZX Spectrum.

H: En Hispasec conocimos a Cuartango, el descubridor de vulnerabilidades en el navegador de Microsoft, en 1998. Antes de entonces, ¿cuál era tu especialidad profesional?, ¿qué trabajos desempeñabas?

JCGC: Siempre he trabajado en temas de comunicaciones informáticas en grandes fabricantes como consultor y desarrollador.

H: ¿Cuál fue tu primer contacto con Hispasec? ¿Estás suscrito a una-al-día?

JCGC: Mi primer contacto con Hispasec sería en 1999, la verdad es que por aquella época no había casi nada en castellano sobre seguridad. Desde entonces sigo leyendo puntualmente el una-al-día. Por cierto aprovecho para desearos feliz cumpleaños a todo el equipo de Hispasec.

H: ¿Cuándo y cómo encontraste la primera vulnerabilidad en Internet Explorer?

JCGC: La primera vulnerabilidad en 1998 era visual ya que era posible falsificar ventanas para hacer pulsar al usuario el botón equivocado. Los avisos de Windows estaban mal diseñados, de hecho siguen estando mal diseñados.

H: En las posteriores vulnerabilidades que detectaste en el navegador de Microsoft, ¿seguías algún tipo de proceso o metodología para su descubrimiento? ¿cuánto de esfuerzo (de dedicarle horas) y/o genialidad (intuición)?

JCGC: Solo el olfato y ninguna herramienta ni método.

H: ¿Cómo era tu relación con Microsoft en el momento de los descubrimientos continuos? ¿Trabajabas con ellos para solucionarlos o esperabas tranquilamente el parche? ¿Alguna anécdota que contar?

JCGC: Yo les pasaba la información y esperaba el parche y después publicaba los detalles. Una vez me

preguntaron en Navidad si me gustaba más el güisqui porque querían regalarme una botella. Les contesté que era de muy mal gusto la pregunta al menos para nuestra cultura española así que les dije que en tales condiciones no podía aceptar ningún regalo de ellos.

H: Durante aquellos años también destacó Georgi Guninski como descubridor de vulnerabilidades en navegadores, raro era el mes que no se publicaba una nueva vulnerabilidad suya o tuya. ¿Cómo era tu relación con Guninski (si es que existía)?

JCGC: De vez en cuando intercambiábamos mensajes incluso en alguna ocasión nos intercambiamos información para discutirla técnicamente.

H: ¿Qué opinas del debate "full disclosure" o revelación responsable?

JCGC: Me parece el tratamiento adecuado para los problemas de seguridad.

H: A día de hoy existen mercados, tanto negros como iniciativas legítimas y reconocidas, en el que se venden y se compran las vulnerabilidades. ¿Existía algo parecido en la época en la que estuviste más activo en el descubrimiento de vulnerabilidades? ¿Podía ser entonces una actividad directamente rentable en términos económicos o sólo en imagen y prestigio? ¿Tuviste ofertas para comprar tus próximas vulnerabilidades?

JCGC: Yo nunca tuve ofertas ni blancas ni negras, tan solo en una ocasión cuando descubrí un agujero del Netscape me enviaron una camiseta y un cheque de mil dólares, ahora que ya está prescrito (pues hace ya casi 10 años) puedo confesar mi pecado. No declaré el cheque a Hacienda, solo lo ingresé en Caja Madrid, esa ha sido mi única trampa a hacienda en 25 años de experiencia como contribuyente.

H: Tras varios años con una gran actividad en el descubrimiento de vulnerabilidades, al menos en el terreno público, no volvimos a tener más "agujeros" ni "ventanas" de Cuartango ¿por qué?

JCGC: Todo cansa.

H: Ahora hay una hornada nueva, de gente muy joven, en el terreno de la seguridad y el descubrimiento de vulnerabilidades. ¿Algún consejo para ellos?

JCGC: Que se dediquen a otra cosa.

H: ¿Qué sistema operativo y navegador utilizas? ¿Algún programa de seguridad adicional como antivirus?

JCGC: Personalmente utilizo Windows XP y Explorer. Como antivirus Kaspersky. ¡ Viva el vino, las mujeres y las Windows ! (Espero que no se considere machista lo dicho)

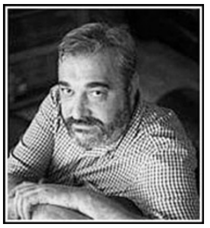
H: ¿A qué dedicas más tiempo últimamente? ¿Hobbies?
JCGC: Mi afición desde hace unos años es la astronomía, los agujeros negros (aunque no se vean, son mucho más interesantes que los agujeros de los ordenadores). Por otra parte la contemplación de la luna creciente de 6 días es mucho más relajante que la contemplación de los pantallazos azules.

H: Un libro, una canción.

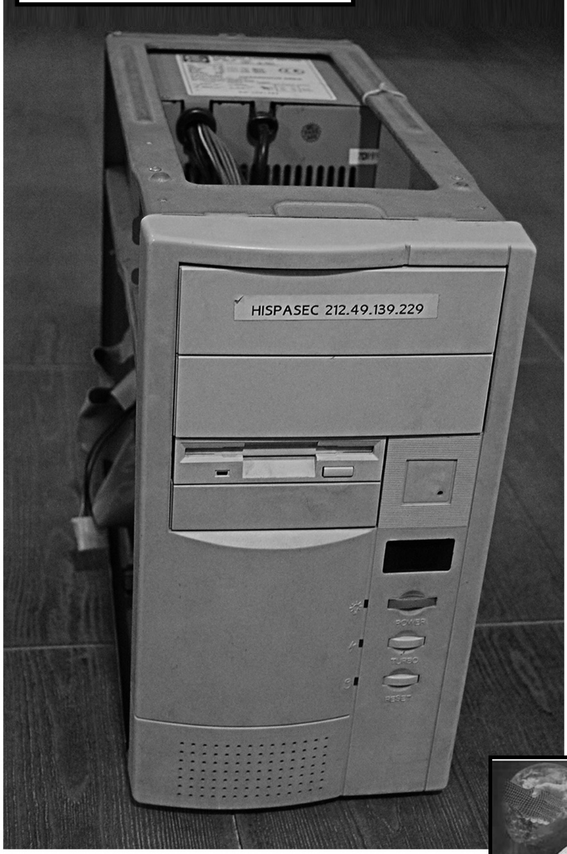
JCGC: Lo que leo en el metro estos días: “La quinta mujer” de Henning Mankell. Canción : “Bye bye miss American pie”

H: ¿Alguna predicción en materia de seguridad informática? ¿Qué nos espera?

JCGC: En 19 años no ha habido ningún avance. Cada vez los ordenadores hacen menos cosas sin advertirte ocho veces sobre el peligro de lo que vas a hacer. Windows Vista y su UAC, o el “sudo” de linux son el paradigma de los avances logrados en 10 años. Parece que nos espera más de lo mismo: tú haz lo que quieras pero yo ya te había avisado así que no soy responsable de nada. En realidad la informática en general no ha avanzado nada en los últimos 30 años.



Primer servidor de Hispasec



Alojaba la primera página web. Sus características:

. Procesador Cyrix 486 DX2 80,
. 16 Mbytes de RAM,
. Disco duro de 6 Gbytes y Windows NT 4.0.

Estaba directamente conectado a internet, sin cortafuegos físico o por software.

Primera página web de hispasec



Capítulo

1

AÑO 1999

7CF

3717

11111001111



915148800 – 946684799

Durante este año...



_ En la Unión Europea entra en vigor el **euro** como moneda única en 12 estados. El dinero físico se pondría en circulación a principios de 2001.

_ En enero se lanza la **Mars Polar Lander**. Fue una sonda espacial estadounidense que despegó en enero y llegó a su destino en diciembre de 1999. Es el primer intento de amartizaje desde el éxito de Pathfinder en 1997. El 3 de diciembre de 1999, diez minutos antes de aterrizar, se perdería el contacto.



_ El asunto de **Bill Clinton** sigue coleando. Comienza el juicio.

_ Teleline ofrece ahora por 20.000 pts. (120 euros) conexión a un año pero con **módem de 56kbps**. Añade 5 megas de página web y 3 buzones de correo.

_ En abril se produce la masacre en el instituto **Columbine**. Eric Harris y Dylan Klebold, dos adolescentes de Littleton (Colorado) disparan contra sus compañeros y profesores, matando a 13 personas y suicidándose más tarde. Michael Moore lo tomaría como referencia para su película-documental Bowling for Columbine, en una reflexión sobre el uso de armas de fuego en los Estados Unidos.

_ En mayo aparece **Microsoft Windows 98 Second Edition**. Se trata de una actualización como consecuencia de la pérdida del juicio antimonopolio por la integración del navegador en el sistema operativo. Podía ser visto como un Service Pack para Windows 98. Actualizaba el navegador a Internet Explorer 5.0 (que ahora podía desinstalarse oficialmente, o al menos hacerlo desaparecer del escritorio, cosa imposible con otras versiones), mejor soporte para USB, DVD y la corrección de otros muchos problemas menores.

_ La agenda electrónica más pequeña del mundo tiene **256 kilobytes de memoria**.

En junio nace **Napster**, lo que supondría la primera revolución de compartición de archivos y redes de pares en Internet. Se convertiría en un programa tremendamente popular y la industria arremetería contra él hasta detener por completo el proyecto. En 2001 alcanzaría su máxima popularidad. Se trata de una red centralizada para mantener la lista de usuarios conectados y archivos compartidos por cada uno de ellos. Sin embargo las transferencias de archivos son realizadas entre los propios usuarios sin intermediarios. No permitía "resumir" por lo que se podía perder un archivo por completo aunque se hubiese descargado al 99% si se cortaba la conexión. Tras varios juicios y demandas que no harían más que elevar su popularidad, en julio de 2001 un juez ordenaría el cierre de los servidores Napster. En mayo de 2008 Napster resurgiría bajo el reclamo de tienda de MP3.

_ En junio Apple comienza a comercializar su **iBook** con CPU PowerPC G3 entre 300 y 466 Mhz. La

primera versión viene equipada con 288 MB de RAM y 3 gigas de disco duro. Se aplica el exitoso diseño de los ordenadores de sobremesa, con unas formas innovadores y colores translúcidos. Cuesta más de 260.000 pts. (unos 1.500 euros) Un poco más tarde ese mismo año aparecería el Power Macintosh G4.



_ En la una-al-día del 15 de mayo, "Galadriel, una semana después " se comienza a incluir el **título de la noticia en el asunto** del correo enviado.



_ Se decide que el euro valdrá **166,386 pts**.

_ Es un año especialmente virulento en cuestión de **terremotos**. 17.000 personas mueren en agosto en Turquía. Este país sufriría más terremotos ese año. También temblaría la tierra de Grecia e incluso España.

_ Silicon Graphics lanza **VirualWorkstation** 540. Permite 4 procesadores Xeon Pentium II a 450 Mhz y hasta 2 Gigas de memoria. Cuesta cerca de un millón de pts. (6.000 euros).

_ **Philip Morris** es condenada por un jurado de San Francisco a pagar 7.250 millones de pesetas (43 millones de euros) a una fumadora con cáncer de pulmón irreversible.

_ En octubre, se establece simbólicamente que el mundo llega a estar habitado por **6.000 millones de personas**. La población crece indiscriminadamente desde el final de la segunda guerra mundial y continúa hasta nuestros días. En 1950 sólo existían 2.000 millones de seres humanos. En 2008 somos 6.700 millones. Se esperan los 9.000 millones para 2042. En España somos 40 millones en 1999 y 46 en 2008.

_ Las memorias **Compact Flash** alcanzan los 160 megas. Un escáner 600x1200 cuesta casi 20.000 pts. (120 euros). Una grabadora Yamaha 6x2x2x (lee a 6 velocidades, graba y regraba a 2) cuesta 300 euros (50.000 pts).

_ Se lanza **FreeBSD versión 3** y **OpenLinux 1.3**.

Seguridad Informática



_ Se descubre uno de los primeros **troyanos que roba** cuentas de usuarios de America Online. Se añade al fichero win.ini para asegurarse la ejecución en cada inicio. El troyano viene en forma de archivo ejecutable y "cifra" a través de una simple transposición de caracteres los datos robados, que son enviados a una dirección de correo en China. Durante todo el año se descubrirán muchos más, destinados a robar las contraseñas para permitir la conexión gratuita a Internet a través de AOL y otros proveedores.

_ Un analista de SecureXpert da a conocer una **vulnerabilidad que afecta a todos los navegadores**. La vulnerabilidad permite al autor de una página especialmente manipulada o un mensaje correo HTML, falsear la información presentada por otro sitio web. El problema es común a Microsoft Internet Explorer y a Netscape Communicator, y se debe a que ambos navegadores no pueden evitar que un sitio web pueda

reemplazar un frame mostrado por otro sitio web con contenido que está bajo el control del atacante. El fallo se descubrió primero en Internet Explorer y más tarde se observó que el resto también eran vulnerables. Todavía estos métodos no serían usados para el phishing, un concepto que llegaría mucho después, al igual que un buen número de vulnerabilidades parecidas compartidas entre los navegadores actuales.

_ La colegiala irlandesa **Sarah Flannery** de 16 años, desarrolla un algoritmo de clave pública basado en matrices 2x2, con el que consigue un cifrado fuerte comparable a RSA y 30 veces más rápido. Sarah no piensa patentar el código. Su padre comenta que "a ella no le importa el ser rica, lo que realmente desea es hacer partícipe a todo el mundo de la felicidad que le ha proporcionado su descubrimiento". Lo llama Cayley-Purser en honor a Arthur Cayley, un experto en matrices de Cambridge del siglo XIX, y a Michael Purser, un criptógrafo del Trinity College, en Dublín, quienes inspiraron a Sarah en su desarrollo. Publicaría un libro en 2001 y posteriormente se descubriría que su algoritmo contenía un error fatal, aunque esto no lo descartaba totalmente para poder ser usado bajo ciertas circunstancias. Actualmente Sarah trabaja en Electronic Arts.

_ Tras el virus Strange Brew, la plataforma Java se ve afectada por el virus **BeanHive**, mucho más sofisticado que su predecesor. BeanHive está destinado a conseguir acceso total a los datos de los usuarios a través de su ejecución en los navegadores.

_ **Intel llega a un acuerdo con la RSA** para dotar a sus futuros procesadores de capacidades para el cifrado de datos. Se habla de que esta tecnología permitirá facilitar en gran medida el uso del cifrado en red e impulsar el comercio electrónico, una gran apuesta en aquel momento.

_ **El desafío DES III** se rompe en el tiempo récord de 22 horas y 15 minutos, gracias al poder de unos 100.000 ordenadores y un superordenador especialmente diseñado por la EFF (Electronic Frontier Foundation) conocido como "Deep Crack". En esta ocasión el ya mítico ordenador, (que ganó por sí solo el anterior concurso en menos de tres días) colaboraba con distributed.net, y en combinación se probaban 245.000 millones de claves cada segundo. Se demuestra en primer lugar la debilidad del algoritmo DES y la necesidad de buscar un nuevo sustituto de forma inmediata (se propuso AES) y por otro lado la efectividad del uso de la informática distribuida para la resolución de problemas que requieran una gran potencia de cálculo. El escrito tras la clave oculta la siguiente misiva "See you in Rome (second AES Conference, March 22-23, 1999)". RC5-64 caería tres años después.

_ Durante el transcurso de la Conferencia de Seguridad de Datos de la RSA en San José, compañías como IBM o Netscape se decantan por la implantación y el uso del **estándar PKI**. El estándar PKI (Public Key Infraestructure) desarrollado por la Internet Engineering Task Force (IETF), está basado en el uso de clave pública y pretende asegurar que tanto el receptor como el emisor de un mensaje son realmente quienes dicen ser. Además, PKI garantiza que la integridad de los datos no ha sido comprometida. Representa el primer apoyo firme por parte de la industria para su implementación. Entre las diferentes medidas adoptadas por IBM se encuentra la migración de 30 millones de usuarios de Lotus Notes (principal competencia de Office en el momento) al estándar PKIX (PKI sobre X.509). En esos momentos no existían muchas aplicaciones que soportasen o hicieran uso del PKI.

_ **Juan Carlos García Cuartango** descubre una vulnerabilidad en Internet Explorer por la que se deja visible el portapapeles en Internet. Las reglas de seguridad de Microsoft dejan clara la prohibición del acceso al contenido del portapapeles a los scripts de Internet Explorer a no ser que sea propiedad del propio Explorer, pero existe un medio para evadir esta protección a través del uso de algunos controles ActiveX incluidos en MS Forms 2. La vulnerabilidad también puede ser aprovechada por correo. Cuartango

descubre más tarde que no es necesario usar el ActiveX. Años después este problema del portapapeles seguiría coleando con Internet Explorer.

_ Según el CERT, algunas de las copias del código fuente de **TCP Wrappers** han sido modificadas para incluir en ellas un troyano, que daría la posibilidad a un intruso a entrar en un sistema remoto por el puerto 421 con permisos de root. Una vez compilado este troyano es capaz de mandar información a una dirección de correo externa, como la identificación del lugar y de la cuenta que lo ha compilado.

_ El proyecto Katmai se materializa comercialmente en **Pentium III**. Se dice que incluirá importantes medidas para fortalecer la seguridad y mejorar las condiciones del comercio electrónico. Se modifica el generador de números aleatorios, hasta ahora basado en software, a pesar de que todos los criptoanalistas confirman las debilidades de este medio para crear números aleatorios. A la larga pueden emerger patrones numéricos, llegar a predecirse el numero pseudoaleatorio y por lo tanto descifrar el mensaje. El generador que se incluirá en el Pentium III determinará el número calculando la diferencia entre el ruido térmico emitido por al menos dos puntos del procesador.

_ El chat hace furor en la red, y es una de las actividades más realizadas en Internet. mIRC 5.5, el programa cliente IRC en Windows por excelencia, se convierte en una importante puerta de entrada para **troyanos a través de comandos DCC**. El DCC también sirve como vía de contagio para los virus-scripts de mIRC, que aprovechan que por defecto los archivos aceptados por DCC se almacenan en el directorio junto con los ficheros de scripts.



El tema estrella del año es el **"efecto 2000"**, pero también se avisa de que la entrada del Euro (al menos al año siguiente entraría como moneda de curso en los mercados bulsátiles, no llegaría a los bolsillos hasta 2001) también podría causar problemas. A primeros de año un gran número de informáticos se ven obligados a hacer horas extras par adaptar todos los sistemas a la nueva moneda europea. Se piensa que los fallos que traerá consigo no permitirán que se baje la guardia durante mucho tiempo y que los tres próximos años serán susceptibles a la aparición de errores y problemas con igual probabilidad a la de cualquier otro día. Microsoft retira del mercado toda su serie de programas de contabilidad doméstica Money 99 por un problema de adaptación de la nueva moneda con la banca online. Money 99 incluye unos scripts para la conversión, pero estos se muestran incapaces de acceder a los servidores bancarios alemanes a pesar de ser compatibles. La línea de soporte de la compañía recibe más de 500 llamadas diarias con relación al Euro y el Money 99.

Durante todo el año, la CIA sigue alarmando sobre el problema del año 2000. El nuevo milenio podría causar serios problemas en algunos países en los sistemas de misiles, suministros de agua y gas, reactores nucleares, etc. El vicesecretario de defensa estadounidense, John Hamre, anuncia que según los informes de inteligencia en su poder, son posibles dificultades en los envíos de gas en la antigua Unión Soviética. Los países en vías de desarrollo como China podrían sufrir con mayor virulencia la entrada del milenio con probables daños en sectores como telecomunicaciones, electricidad y banca. Los países árabes podrían no ser conscientes del bug del 2000 porque se rigen por un calendario musulmán. Los Estados Unidos hacen culpables de los posibles fallos de sus

sistemas a la falta de previsión de los países aliados. La Comisión del Senado que estudia el problema dice al respecto "Los estadounidenses deben prepararse para el problema del año 2000 en los ordenadores como lo harían de cara a un huracán, almacenando alimentos enlatados y agua embotellada". La fantasía sobre el efecto 2000 alimenta películas, series y todo tipo de artículos catastrofistas.

En España siguen publicándose estudios acerca del año 2000. Según afirman fuentes del gobierno, un 85% de los sistemas informáticos de la administración están dispuestos para afrontar el año 2000 sin errores. En agosto se crea la Oficina de Transición para el Efecto 2000. Este nuevo centro de coordinación viene a sustituir a la Comisión Nacional del Efecto 2000, y el periodo de coordinación será de seis meses que comprenderán entre octubre de 1999 y marzo del 2000. Sectores como el nuclear y el de transporte marítimo están preparados totalmente para el efecto 2000 y otros como los de hidrocarburos poseen una adaptación del 95%. Otro sector con altos índices de preparación es el de ferrocarriles, con una adaptación del 93%, mientras que la banca con un 90% parece que tampoco tendrá problemas para tenerlo todo a punto para el 31 de diciembre. El panorama más inquietante viene por parte de la sanidad pública que sólo dispone de un 50% de sus ordenadores preparados. Otro problema añadido es el de las Comunidades Autónomas: el 30% no ha comenzado la adaptación. El intercambio de información entre administraciones nacionales y autónomas puede dar al traste con los ya preparados ordenadores del Estado. No sería para tanto.

_ Cisco, Lucent, NAi y Sun, firman un acuerdo para unir sus fuerzas a favor de la protección de los usuarios. Se crea la **Security Research Alliance** para compartir avances en sus investigaciones, así como colaborar en el desarrollo de nuevos medios y aplicaciones que garanticen la defensa de los sistemas informáticos. La alianza tiene como meta proporcionar a los administradores la información que necesitan para tomar decisiones a largo plazo. También, en la cabeza de la lista de prioridades de la Alianza se encuentra la detección de intrusos y la respuesta ante este tipo de incidentes. La mayoría de los sistemas de detección de intrusos fijan su atención en la capa de aplicación, pero la Alianza quiere llegar a ser capaz de detectar ataques a una organización desde el nivel más bajo de las capas IP hasta en los niveles altos de aplicación. Con la perspectiva del tiempo, el efecto real del proyecto en la seguridad no sería demasiado destacable.

_ Bajo el nombre de **Linux.Vit.4096** se anuncia la aparición de un nuevo virus que afecta al sistema operativo Linux, no residente en memoria y capaz de replicarse en ejecutables con formato ELF. El proceso de infección lo lleva a cabo insertando su código (4096 bytes) después de la cabecera ELF en la primera sección de código del fichero. La primera noticia que se conoce sobre virus para Linux se remonta a septiembre de 1996, cuando en algunas news se difundió en un mensaje la versión alpha de Bliss, considerado como el primer virus para Linux. Por aquel entonces fue McAfee el primer antivirus en sacar su antídoto al mercado. Los productos antivirus para Microsoft añaden este virus a sus firmas.

_ Un nuevo virus de macro (tipo favorito de virus durante todo 1999), **W97M/Caligula**, roba los ficheros de claves del programa de cifrado PGP. Un ataque posterior a estos ficheros por fuerza bruta podría permitir abrir los archivos cifrados. Copia el fichero secreto de llaves de PGP (SECRING.SKR) y lo enviaba a través de FTP al servidor de su creador. Parece que la única razón por la que este virus roba el fichero de PGP es para convertirse en el primero con esta característica y obtener así la máxima notoriedad. Un ataque más efectivo podría llevarse a cabo introduciendo capacidades de "keylogger". En 2008 se detectaría otro troyano que robaba claves PGP y obtendría una repercusión mediática parecida.

_ En febrero se detecta **el primer virus que elimina virus**. W97M.Ethan funciona de forma similar a la mayoría de virus de macro y sólo infecta ficheros de Word. Ethan borra el archivo class.sys, en el que se esconde el virus de macro W97M.Class. Años más tarde se observaría una guerra vírica en la que varios tipos de malware se centraron en eliminarse mutuamente.

_ La administración de Estados Unidos sigue intentando restringir la exportación de productos criptográficos. WatchGuard Technologies recibe el permiso para la **exportación de software de cifrado de 128 bits**. La concesión otorga libertad para exportar el componente Virtual Private Network (VPN, Red Privada Virtual) del Sistema de Seguridad WatchGuard (WatchGuard Security System) a 41 países. Esto sienta un precedente en la exportación de material criptográfico.



La polémica viene de la mano de Intel y su nuevo **Pentium III** por la decisión de incorporar un **número de identificación** a todos los chips. Este número conocido como PSN (Pentium Serial Number) ofrece la posibilidad de acceder a él desde las aplicaciones. Intel justifica la inclusión alegando su utilidad para las transacciones electrónicas. La medida del número identificativo no convence a una gran parte de los usuarios. Para acallar las quejas, Intel opta por ofrecer los chips con dos posiciones para el acceso al código. Por defecto, los procesadores se distribuirán con la característica cerrada, dejando al usuario la decisión de activarla mediante un programa proporcionado por la propia compañía. Intel asegura que no sería posible acceder al número de serie si el usuario deja desactivada dicha opción, pero la revista CEBit anuncia que uno de sus ingenieros ha desarrollado un programa capaz de acceder al número de serie incluso sin que el usuario lo haya permitido. Se pone a disposición de todos la web http://www.zks.net/p3 para que a través de ActiveX se pueda leer el famoso número de serie de Pentium III. Si se puede acceder por software sin permiso del usuario, también será posible modificarlo, o devolver un número falso cuando se solicite. Se crea una campaña anti-Intel, mofándose de su logo http://www.bigbrotherinside.com/. En diciembre de ese mismo año, el Parlamento Europeo, aconsejado por un grupo de expertos en seguridad informática, se plantearía la posibilidad de prohibir la instalación de procesadores Intel Pentium III en Europa. Finalmente, la polémica terminaría en marzo de 2000, cuando Intel decide eliminar el número de serie en su próxima familia de procesadores.

_ Aparece un gusano con múltiples técnicas reproductoras. **IRC-Worm.Septic** es capaz de reproducirse por múltiples vías, desde el IRC, hasta los ficheros html o los BAT.

_ Se publica la nueva versión de **NetBus Pro, la 2.0**. Los troyanos de acceso remoto a través de un puerto abierto en la víctima están en pleno auge. NetBus rivaliza en popularidad con el conocido Back Orifice. El troyano permite la obtención de información de los sistemas remotos, caché de contraseñas, subir y bajar ficheros, capturas de teclado y pantallas del ordenador remoto o la posibilidad de incorporar plug-ins. NetBus permite ahora escuchar a través del micrófono, capturar desde dispositivos de video (webcams), acceso y edición del registro, chatear y hasta la incorporación de un programador de tareas para ejecutar scripts en un momento determinado sin necesidad de que el cliente “atacante” esté conectado. NetBus Pro 2.0 incorpora soporte multilingue y sólo pesa 1.7 megas. El puerto TCP que utiliza para escuchar las conexiones es el 20034. En hexadecimal obtendremos 4E42, y estos dos bytes pasan a ser en ASCII “NB”, iniciales de NetBus. Más tarde, Back Orifice anunciaría su nueva versión durante la convención de temática underground Undercon 7, celebrada en julio en Las Vegas. Cult of Dead Cow (Culto de la vaca muerta) presenta la Back Orifice 2000 (o BO2K).

_ En marzo se descubre que **Windows puede bloquearse pasados 49,7** días de uso continuado. Microsoft ofrece un parche para solucionar este problema. Son muchos los usuarios que ante este anuncio se preguntan en qué condiciones ha conseguido Microsoft mantener una máquina con estos sistemas operativos funcionando mes y medio de forma continuada para poder reproducir el fallo.

_ Los sistemas informáticos estadounidenses siguen sufriendo ataques de **hacktivistas**. Curt Weldon representante del Departamento de Defensa de los Estados Unidos, lleva a cabo una investigación sobre estas intrusiones. Los intentos de introducirse dentro de los sistemas informáticos de la defensa norteamericana se realizan de forma coordinada y organizada. Según el Pentágono, Rusia ha sido el origen de estos ataques. Weldon añade "podríamos decir que estamos en guerra".

_ Microsoft admite el uso de un **número identificativo en Word y Excel** que permite reconocer de forma única a los autores de estos documentos. La confirmación sale a la luz justo durante la polémica existente con el número de serie de los Pentium III, por lo que Microsoft reconoce rápidamente la amenaza a la intimidad de los usuarios que constituye este código. Dice que se trata de un error de programación y que será solucionado en la próxima Service Release de Windows 98. Para aquellos usuarios que ya tienen instalado el sistema operativo, la compañía ofrece una utilidad para desactivarlo.

En marzo irrumpe **Melissa** y los medios se vuelcan. Llega la época dorada de los virus de Macro, basados en documentos Office. Es tal su propagación que llegaría a colapasar los sistemas de correo con emails infectados. Aunque no fue diseñado en primera instancia para provocar daño alguno, causa el caos en la red. Se distribuye a través del grupo de discusión alt.sex, dentro de un fichero .DOC que contiene contraseñas para acceder a páginas pornográficas de pago. Aparecerían posteriormente decenas de variantes, como por ejemplo el virus de macro Papa que se basa en su código.

Hispasec realizaría en su una-al-día del 28 de marzo de 1999 un extensísimo análisis sobre este especimen.

_ Un error en los Kernel Linux inferiores a 2.0.36 posibilita ataques **IP Spoofing de forma trivial**, sin necesidad de tener acceso a la red local de la máquina atacada, ni de realizar predicción de números de secuencia TCP. Muchas pilas TCP implementadas en aquellos momentos, ofrecían números de secuencia de paquetes correlativos, favoreciendo ataques que permiten el envenenamiento de tráfico.

_ Se designa el **AES (Avanced Encryption Standard)** como algoritmo que sustituye a DES. El NIST (National Institute of Standards and Technology) es el encargado de la elección del método de cifrado destinado a convertirse en un estándar internacional. Los mejores criptógrafos creen que el AES durará como estándar unos 50 años. En marzo la RSA patenta un sistema para interactuar entre criptosistemas de curvas elípticas, lo que se supone será el futuro de la criptografía.

_ Se lanza **Internet Explorer 5.0** y reaparecen los agujeros de Cuartango. Guninski descubre un nuevo fallo que permite leer y enviar ficheros locales a un servidor remoto. Se descubre que durante la instalación se modifican las propiedades en el salvapantallas sin avisar al usuario, lo que podría acarrear problemas en la seguridad a nivel local en determinadas configuraciones. Durante los siguientes meses Cuartango y Guninski seguirían encontrando vulnerabilidades en el navegador.

_ En abril se descubre que los ordenadores PC Aptiva de la serie 240, 301, 520 y 580 fabricados por IBM

entre los días 5 y 17 de marzo de 1999 pueden estar **infectados por el virus CIH**.

_ Un agujero basado en JavaScript permite que usuarios de **eBay**, el famoso sitio de subastas, roben contraseñas de otros miembros legítimos. Cualquier usuario del sistema que utilice un navegador con JavaScript habilitado puede ser víctima. El fallo se debe a que existe la posibilidad de incluir código JavaScript como parte de las descripciones de los objetos que se proponen a subasta.

_ La policía taiwanesa no toma ninguna acción contra el joven programador del **virus CIH**. Por el contrario, se dice que el creador de Melissa podría ser condenado a una pena de hasta 40 años de prisión.

_ En mayo Hispasec descubre el **primer virus para Corel Draw**, GaLaDRieL. Basado en Corel Script, el lenguaje de programación para la automatización de tareas y guiones de Corel Draw. No tiene efectos dañinos. Ante el anuncio público y exclusivo de Hispasec, la reacción que demuestran las casas antivirus y los medios en general es diversa. Desde las que solicitaban una muestra del virus, pasando por las que se apresuran en hacer llegar sus actualizaciones para combatirlo, hasta las menos afortunadas que piden un fichero binario infectado.

_ Se descubre el virus **Girigat**, cuya principal característica es su capacidad de automutar: su forma de funcionar varía cada vez que cambia de ordenador. El virus puede ser residente por proceso (por medio de API "hooking") o "runtime", o incluso ambos. También, en caso de funcionar por medio de acción directa, es capaz de trabajar o bien en el directorio actual, o bien en el de Windows, o bien en ambos. Por último, Girigat es capaz de infectar CPL (paneles de control), EXE (ejecutables PE) y SCR (salvapantallas). Puede resultar en 63 variantes distintas de un mismo malware. Los creadores de malware se lucen con especímenes muy sofisticados.

_ Las boyante escena vírica española del momento crea **Veneno**, un virus de macro para la versión española de Word, a la zaga de Melissa y Papa. Luego aparecería ZippedFiles, también aprovechando el código de Melissa.

_ En mayo nace **HushMail**, un proyecto de éxito que perduraría hasta nuestros días y que proporciona privacidad, mediante un sistema de cifrado de llave pública, a través de un cliente de correo vía Web usando un applet de Java. Se presentan como la alternativa a otros sistemas que resultan más complicados a la hora del intercambio de claves criptográficas, el coste del software y las limitaciones que supone las leyes de exportación de los EE.UU.

_ También en mayo Hispasec inaugura su **servidor de llaves PGP** basado en LDAP (Lightweight Directory Access Protocol). Se comienzan a firmar criptográficamente las noticias.

_ En junio se hace público un grave agujero de seguridad en **Internet Information Server 4.0** para Windows NT 4.0. eEye Digital Security Team advierte del peligro de la existencia de un problema de desbordamiento de memoria intermedia que permite la ejecución de código. El exploit es trivial y público. Si se envía una orden "GET /[sobrecarga].htr HTTP/1.0", donde [sobrecarga] es una cadena de unos 3 Kbytes, el Internet Information Server trata de leer la página solicitada, pero la isapi.dll (por defecto en todos los IIS) no realiza una comprobación apropiada. El agujero despierta el interés de todos, son millones los servidores vulnerables. eEye publica un parche no oficial. Microsoft lanza un comunicado. Muchas páginas web amanecen desfiguradas. Microsoft publica la actualización oficial tres días después del descubrimiento.

_ Julio César Hernández, consultor de IP6 Seguridad, descubre **WinSATAN**, un nuevo troyano que resulta una versión para Windows de la herramienta de auditoría de seguridad para Unix SATAN.

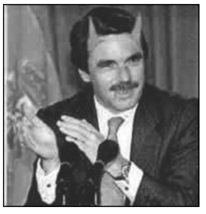
_ Las conexiones por cable y **ADSL** se popularizan gracias a las primeras ofertas de tarifa plana y router gratis. En aquellos momento se obtenía una dirección IP fija por defecto y sin pagar más por ello. Se alerta sobre los potenciales peligros de la conexión permanente con una dirección fija, que favorece un seguimiento del usuario al que se pretende atacar.

_ Las pilas TCP de Windows no toleran cabeceras IGMP mal construidas. Cuando se recibe un paquete de tales características, la pila falla de forma impredecible, con resultados como un clásico bloqueo con la pantalla azul o un reinicio automático. Se descubre un nuevo **"ping de la muerte"**.

_ En junio salta la polémica a causa de un **grave problema de seguridad en Hotmail**, el servicio de cuentas de correo gratuitas más empleado del mundo. En julio, Georgi Guninski descubre un medio por el que se puede conseguir robar la contraseña del usuario que se desee. Descubriría todavía algún otro método más durante el año. En agosto dos sitios web, uno en el Reino Unido y otro en Suecia, permitían acceder a cualquier cuenta de Hotmail conociendo su nombre de usuario, sin necesidad de suministrar la contraseña. El correo confidencial de los cerca de 50 millones de usuarios de Hotmail ha estado a disposición de cualquiera. www.lettera.net, el popular webmail ya desaparecido, sufriría el mismo problema meses después.

_ En julio se descubre que el **sistema de cifrado en MacOS** es bastante débil. La combinación de los valores hexadecimales que componen la contraseña a través de sencillas operaciones XOR, junto con valores fijos, bastan para realizar la inversión del cifrado.

_ La quinta encuesta anual sobre la influencia de virus informáticos realizada por la ICSA refleja interesantes datos sobre el **incremento de las infecciones víricas en los últimos meses**, a pesar de que la mayoría de ordenadores y servidores tienen instalado algún tipo de software antivirus. En enero y febrero de 1999 el porcentaje de infecciones por mes y por cada cien ordenadores es el doble que la tasa de 1998 y cuadriplica la de 1997. La encuesta es realizada entre 300 compañías americanas y organizaciones gubernamentales con un total de más de 800.000 ordenadores representados. También se refleja el aumento en el uso de software antivirus, un 83 % de los entrevistados tienen al menos un 90% de los PCs protegidos con software antivirus. La mayoría de los PCs (60%) están protegidos en todo momento con algún tipo de antivirus residente. En torno a un 43% de los entrevistados ha sufrido algún desastre por infección vírica en algún momento, con un índice de más de 25 ordenadores infectados al mismo tiempo. Y una gran mayoría, un 80%, ha tardado más de 50 horas en recuperarse de un ataque de este tipo. Toda la encuesta refleja la importancia de la protección antivirus, así como la actualización del software y la educación de los usuarios.



_ En agosto **la página oficial de la Moncloa sufre un ataque** y modifican una fotografía del presidente de aquel momento, Jose María Aznar, añadiéndole cuernos y una boca chorreando sangre. "España NO VA BIEN", escribieron además los atacantes.

_ Hispasec descubre el sistema de **cifrado de WS_FTP**, un popular cliente FTP.

_ **Nace MSN Messenger**, el exitoso intento de Microsoft por derrocar al imperante ICQ del momento en el campo de la mensajería instantánea. MSN Messenger Service 1.0 nace sin versión en español y reduciendo drásticamente el tamaño y los recursos necesitados por ICQ. MSN Messenger se trata de un

diminuto ejecutable de 324kb. ICQ ya pesaba varios megas en 1999. A finales de año se descubriría que almacenaba las contraseñas con cifrado débil.

_ En octubre RealNetworks admite que una de sus aplicaciones, **RealJukebox**, registra los hábitos y actividades de los usuarios. La aplicación envía los datos a RealNetworks sin el conocimiento del usuario. RealNetworks recopila información de más de 13 millones de usuarios registrados de RealJukebox: tipo de música, el formato de los ficheros, o el número de canciones almacenadas en su disco duro. Esta información es acompañada de un número único (GUID) que identifica al usuario y permite a RealNetworks mantener una base de datos con los hábitos individuales de cada uno de los usuarios. La intimidad se ve constantemente amenazada en la red.

_ A final de año Cuartango descubre un **grave fallo en Outlook y Outlook Express**. La vulnerabilidad permite la ejecución de cualquier programa tras abrir, por medio de doble click, un fichero adjunto aparentemente multimedia, que en realidad sería un ejecutable sin advertencia alguna. Microsoft lo corregiría 10 días después.

_ Se hace pública documentación técnica y software para **decodificar y copiar discos DVDs**, saltándose las protecciones criptográficas diseñadas para este sistema, denominadas CSS (Content Scrambling System).

_ En diciembre aparece **Babylonia**, el primer virus autoactualizable por Internet por medio de "plug-ins". Un agente infeccioso que reúne las habilidades de un gusano en cuanto a su distribución, de un virus en cuanto a la infección de ficheros, y de un troyano de "backdoor" en lo que a las actualizaciones se refiere. Sería un comportamiento habitual del malware varios años después.

Una al día

07/01/1999 RSA evita la regulación criptográfica de EE.UU.

RSA Data Security ha abierto una filial en Australia, de esta manera consigue liberarse de las regulaciones comerciales impuestas por los EE.UU. en materia de exportación criptográfica. La RSA fue fundada en 1982 por los inventores del criptosistema de llave publica (RSA PKC), River, Shamir y Adleman. Hoy día la RSA se ha convertido en sinónimo de criptografía, con más de 300 millones de copias de sus sistemas de cifrado y autentificación.

Hasta el momento, la RSA tenía que regular su software teniendo en cuenta la política de la administración Clinton, que impide exportar productos cuyos algoritmos criptográficos superen la barrera de los 56-bit. Según el gobierno de los EE.UU., longitudes más largas hacen los cifrados más difíciles de romper, y en consecuencia podría ayudar a encubrir información a los criminales.

El resultado final es que los que soportan estas restricciones son los usuarios y empresas que se ajustan a la ley. Con respecto a los criminales, parece claro que harán caso omiso de estas restricciones, y por descontado no van a utilizar los algoritmos fáciles de romper para que el gobierno de los EE.UU. pueda tener acceso a su información.

Para evitar estas restricciones la RSA ha instalado en Australia una sucursal, dentro de un ambiente

regulador mucho menos riguroso, donde podrán desarrollar y comercializar software de cifrado fuerte. Los analistas dicen que con este movimiento la RSA consigue un gran avance al poder competir en igualdad de condiciones con sus rivales.

La RSA (www.rsa.com) llevaba varios meses negociando con el Departamento de Comercio de los EE.UU. para cerciorarse de que la nueva empresa australiana no violara el código comercial. Tras estos encuentros, el departamento accedió con la condición de que no se utilizara a ningún empleado ó tecnología de los EE.UU. en la filial australiana.

Para cumplir el acuerdo, la RSA compró una compañía australiana que reconstruyó los algoritmos basándose en especificaciones disponibles públicamente. Con esta medida, la RSA se ahorra el coste que suponía el obtener una licencia comercial para cada producto suyo que superara el cifrado de 56-bit.

SUN Microsystems había intentado, con anterioridad, la misma estrategia a través de la empresa rusa Elvis-Plus, de la que poseía el 10%. En aquella ocasión el Departamento de Comercio de los EE.UU. junto con la Agencia de Seguridad Nacional (NSA) decidieron paralizar el intento de SUN. La NSA requirió y analizó el código fuente de los algoritmos de SUN y Elvis-Plus, determinando que había indicios de la tecnología de SUN en los fuentes de la compañía rusa.

Bernardo Quintero

15/03/1999 Windows 98 un peligro para la intimidad

Cuando todavía está reciente la información acerca de los problemas del número identificativo generado por las aplicaciones más conocidas de Microsoft y que se envía al registrar Windows 98, surgen nuevos avisos de ataque a la privacidad en torno a Windows 98.

Cualquier sitio web puede leer la información que identifica uniquívocamente cada usuario y su ordenador, pero incluso estos datos pueden ser modificados y enviados a Microsoft, todo ello sin el conocimiento ni la autorización del usuario.

Windows 98 hace uso de RegWiz para procesar el formulario de registro del sistema operativo y enviarlo a Microsoft a través de Internet. A partir de la configuración del ordenador y los datos introducidos por el usuario en el formulario de registro se generan dos números que permiten identificar de forma única al PC y al usuario. A través del Número de Identificación de Hardware (hardware identification number, HWID) se puede determinar de forma inequívoca el ordenador del usuario, mientras que a través del Microsoft ID (MSID), se puede precisar el usuario. Este segundo dato se localiza en una cookie para el acceso a los servicios del web de Microsoft.

Pero las funciones de RegWiz van mucho más lejos, ya que permite que tanto el HWID como el MSID queden al alcance de cualquier sitio web, e incluso permite su modificación. Esto quiere decir que cualquier sitio web puede leer los números o por otra parte modificarlos, todo ello sin el conocimiento del usuario. Se puede encontrar una demostración de cómo una página web puede leer y modificar los números en www.winmag.com/web/regwiz.htm.

Todo parece indicar que la problemática es mucho mayor de lo que en principio parecía, ya RegWiz también tiene la posibilidad de enviar toda la información acerca del PC, el hardware y las aplicaciones que se

ejecutan sobre él, a Microsoft sin el conocimiento, ni la autorización del usuario.
Microsoft pondrá a disposición de los usuarios un parche y una herramienta que permitirán borrar todo rastro de estos números de su ordenador y documentos. La compañía también asegura que esta característica estará totalmente desabilitada en el ya inminente Office 2000.

Antonio Ropero

30/03/1999 Problemas en los nuevos navegadores

Tanto Netscape como Microsoft brindan a los usuarios las últimas y más actualizadas versiones de sus navegadores, pero ninguno se libra de los problemas de seguridad. Las dos compañías brindan navegadores más rápidos, más evolucionados y con mejores características, todo con objeto de obtener una mayor cuota de usuarios que su competidor. Pero qué ocurre con la seguridad de los usuarios. A los pocos días de su aparición pública ya se han encontrado errores y problemas en ambos productos.

Georgi Guninski habitual por sus descubrimientos en torno a Netscape ha encontrado el primer fallo propio en la versión 4.51 de Communicator para Windows 95, también existente en la anterior 4.5 y 4.08 para Windows NT. El problema permite espiar y obtener la url que se está visitando en otra ventana del navegador.

Pero los problemas no sólo rodean a Netscape ya que el novedoso Explorer 5.0 de Microsoft sigue inmerso de problemas con relación al portapapeles. Juan Carlos García Cuartango ya detectó varias vulnerabilidades, de las que nos hicimos eco en su momento, en torno a la visibilidad del contenido del portapapeles con Explorer 4. Hemos podido comprobar como algunos de aquellos problemas que estaban parcheados en la anterior versión, no lo están en la edición española del nuevo navegador.

El propio Cuartango avisa sobre un cambio en la política de seguridad de Explorer 5, en el nuevo navegador se pueden realizar operaciones de pegado desde cualquier origen del portapapeles. La conclusión es clara, la política de seguridad de este elemento es menos restrictiva en Explorer 5 que en la anterior versión. Juan Carlos lo advierte claramente, «la realidad es que los usuarios de Internet Explorer 5 están perdiendo privacidad».

Antonio Ropero

13/04/1999 Virus y troyanos indescifrables, a la búsqueda de objetivos desconocidos

Aunque hasta el momento la mayoría de los virus y troyanos que hacen uso de técnicas criptográficas lo hacen con fines exclusivamente de “prueba de concepto” o demostración, en el futuro es previsible que esas mismas técnicas sean empleadas para ocultar el objetivo de esos programas, ya no de los investigadores que intentan analizarlos, ¡¡sino también de sí mismos!!.

Efectivamente, las claves necesarias para descifrar el virus, en la actualidad, están accesibles en el propio código del programa, ya que éste las necesita para descifrarse a sí mismo antes de ejecutar el “payload”. Aunque esas claves pueden estar protegidas mediante intrincadas rutinas cuyo único fin es mantener alejados los ojos curiosos, no pueden ocultarse indefinidamente contra un investigador con medios y

tiempo para afrontar la tediosa la tarea de analizar el funcionamiento del espécimen.
No obstante el estado del arte, en el ámbito criptográfico, permitiría desarrollar programas víricos, caballos de troya, gusanos, etc., protegidos mediante cifrado, pero cuya clave de apertura no aparece en el código, sino en el entorno de ejecución del programa. Ello hace que el código no sólo esté protegido contra miradas indiscretas, sino que ni él mismo "sepa" cuál es su objetivo o qué está buscando... hasta que lo encuentre.

Supongamos un gusano polimórfico. Una vez descifrado el polimorfismo (algo que se puede hacer con conocimientos y experiencia) comprobamos que el programa se dedica a recorrer el disco duro, leer los ficheros que no haya chequeado en la ejecución anterior, dividirlos en porciones de 21 bytes "solapados", y calcular una función HASH sobre ellos.

El resultado de ese HASH se usa como clave para descifra un segmento del gusano. Para verificar si el descifrado es correcto, basta con mantener algún tipo de control de integridad.

21 bytes nos dan 168 bits de entropía. ¡¡Eso es un número de 56 cifras!!.

¿Qué puede estar buscando?. Nunca lo sabremos... ¡¡hasta que lo encuentre!!. Eso es así porque el descifrado solo será correcto cuando dé con lo que busca.

Y como el gusano revisa todos los ficheros del disco duro, independientemente de en qué directorio estén o qué extensión tengan, no tenemos ninguna pista de por dónde empezar. ¿Qué busca?. ¿Un email?. ¿Un programa concreto?. ¿Un número de licencia determinado?. No lo sabemos.

Y lo que es peor... Tampoco sabemos qué acciones hará cuando lo encuentre.

Jesús Cea Avión

03/06/1999 Absuelto el principal acusado del "Caso Hispahack"

"No apareciendo, por tanto, que fuese el acusado quién alteró los programas contenidos en el sistema informático de dicha Universidad, no cabe llegar a otro pronunciamiento que el de su libre absolución". Así termina la sentencia del juez Juan Carlos Llavona Calderón y un capítulo de la historia del "hacking" español, que llevó al banquillo, el pasado 26 de marzo, al principal inculpado, alias JFS, 22 años, administrador de sistemas informáticos y miembro del grupo !Hispahack (!H). El llamado "Caso Hispahack" estalló a primeros de abril de 1998, cuando el grupo de Delitos Informáticos de la Guardia Civil detuvo, acusadas de revelación de secretos y daños informáticos, a cuatro personas apodadas STK, Magne, JFS y JR. Finalmente, la presión judicial se concretó en JFS, para quien el fiscal pedía una pena de dos años de prisión y multa de dieciocho meses, por "un acceso no autorizado a través de Internet" a ordenadores de la Universitat Politècnica de Catalunya (UPC), el 11 de septiembre de 1997. Se descubrió que el intruso tenía privilegios de administrador en dieciseis máquinas, cinco de las cuales tenían instalado un programa sabueso para cazar datos que, aquel 11 de septiembre, el visitante recogió y transfirió a un ordenador de Palma de Mallorca.

Aunque el juez considera estos hechos como probados y, por tanto, no da validez a las reclamaciones del abogado de la defensa, Carlos Sánchez Almeida, sobre nulidad de las pruebas, inexistencia de delito o descriminalización de Internet, sí admite que "tales sospechas no alcanzan la categoría de indicios

bastantes como para desvirtuar totalmente la presunción de inocencia" de JFS. Según la sentencia, no queda probada la identidad del misterioso intruso, se pierde su rastro y, en el ordenador de Mallorca, dice el juez "el acceso se hallaba al alcance de cualquiera que lo hiciese a través del usuario "Hispahack"". Igualmente, recuerda que, según los péritos, "no se hallaba ningún fichero de password (sic) de la UPC" en los ordenadores de JFS.

A pesar del alivio del abogado defensor, quien asegura "el caso !Hispahack ha sido la piedra de toque de la libertad de expresión en Internet en este país. Afortunadamente para el sistema de libertades, el sistema judicial funciona"; la sentencia se muestra firme en algunos puntos que interesarán a la comunidad informática, como la no necesidad de una denuncia previa a la investigación en casos de daños, la afirmación del derecho de las fuerzas de seguridad a obtener datos sobre usuarios de proveedores de acceso sin autorización judicial o la respuesta del juez a las insinuaciones de la defensa de que el "hack blanco" no debería estar penado: "(Son) conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema de que la información que en él se contiene no sea interceptada, resultan tanto más reprobables, y aún merecedoras de sanción penal".

Mercè Molist

29/06/1999 Tres años de virus para Windows9x/NT

Están a punto de cumplirse los tres primeros años desde la aparición de Bizatch (Win95.Boza según la nomenclatura CARO), el primer virus del mundo para plataformas Windows de 32 bits (Windows9x/NT), y parece que es hora de hacer recapitulaciones y estudiar la expansión del fenómeno vírico en este nuevo terreno.

Una nueva plataforma, un nuevo sistema operativo, ha traído como consecuencia la desaparición de ciertos tipos clásicos de virus, y la consiguiente llegada de sus sustitutos naturales. Además es de vital importancia resaltar el hecho de que el cambio ha sido un proceso progresivo y paulatino, una adaptación darwiniana a los nuevos esquemas funcionales.

El cambio más radical ha sido el de la "defunción" de los famosos virus de "boot", que no han sido capaces de encontrar su sitio en Windows, a pesar de haber sido desde siempre números uno en las listas de virus "in the wild" durante la etapa del DOS. El progresivo relevo generacional lo tomaron los virus de macro, que por su sencillez estructural y su carácter multiplataforma han sido una auténtica mina para los escritores de virus que no se manejaban en ensamblador. Dicen que en muchas ocasiones lo más sencillo es lo que triunfa, y en el caso de los virus de macro este dicho se ha hecho bueno: su progresión en cuanto a número ha sido geométrica, y llevan copando, prácticamente desde sus orígenes, los primeros puestos de las listas "in the wild".

Por su parte, los virus de fichero siguen siendo los más "artísticos". Desde la aparición de Bizatch, el primero de la saga, pasó algún tiempo hasta que empezó a darse un flujo normal de producción de virus de estas características. En un principio se trataba más bien de "virus de museo", y así se fueron sucediendo especímenes como Mr.Klunky, Punch, Harry... el paso definitivo de la experimentación a la funcionalidad vino de la mano del escritor de virus peruano del grupo 29A, Jacky Qwerty, el primero en abrir las puertas a los virus al mundo de la compatibilidad Win32, y famoso por haber sido el pionero en numerosas técnicas de programación, como la residencia por proceso.

De esta manera se ha llegado, con el paso de los meses, a una paulatina desaparición de los virus de fichero de DOS, que han cedido el terreno a sus sucesores de Win32. Esto, por otra parte, ha desembocado en una triple vertiente: en líneas generales, los únicos virus de DOS de los que hemos tenido noticia en los últimos meses están caracterizados por un alto nivel técnico, siendo el Emperor el último ejemplo más significativo; por su parte, los virus de Win32 en un principio comenzaron siendo extremadamente "naïve", y no tuvieron que pasar muchos meses para que empezasen a salir a la luz ejemplares de una gran complejidad técnica, de la mano de aquellos escritores de virus experimentados en DOS cuyo proceso de adaptación a Win32 fue un simple cambio de hábitos de programación. Este doble carril ha venido siendo la nota dominante del panorama Win32 hasta el último año aproximadamente, época en la que la situación se ha normalizado, trayendo como consecuencia la predominancia de virus de nivel estándar para plataformas Win32.

Por otra parte, la versatilidad de Windows ha traído consigo la aparición de nuevos tipos de virus hasta ahora desconocidos, nuevas amenazas que, a pesar de haber sorprendido a propios y extraños en el momento de su aparición, no han causado demasiados quebraderos de cabeza a las casas antivirus. Entre los tipos de virus de nueva generación más importantes cabría destacar los dos grupos principales: I-Worms y virus de WSH. Mientras que los segundos no parece que vayan a suponer una seria amenaza, a pesar de ser capaces de infectar HTML y procesos VBS y JS, los primeros están compitiendo en los últimos meses seriamente con los virus de macro en la cabeza de las listas "in the wild".

Los I-Worms son los primeros resultados víricos de la amoldación total a la integración a la red de los ordenadores por medio de Windows: estos agentes infecciosos se limitan a infectar y/o parchear únicamente lo imprescindible, y su mayor amenaza está en su capacidad de reproducirse por medio de la red, o bien valiéndose del e-mail, o bien de mensajes en newsgroups o enviándose por FTP. En el último semestre hemos tenido ocasión de oír acerca de las "andadas" de ejemplares de este tipo como Parvovirus, Happy, PrettyPark o, en la última semana, Zipped_Files. Aparte de éstos, otros dos virus, Melissa y Papa, de macro, también coparon posiciones privilegiadas en los "top-ten" de la ITW, llegando el primero hasta el punto de ver involucrado al FBI en la detención de su autor, un escritor de virus aparentemente desconocido en la escena.

En cualquier caso la rápida difusión "in the wild" no es algo exclusivo de I-Worms y virus de macro: ahí están los ejemplos de, en un principio, Marburg -que llegó a ser distribuido en el CD de un simulador de vuelo y de la conocida revista de difusión europea "PC Gamer"- y HPS, y, en una segunda etapa, el extendidísimo CIH y el versátil Girigat, que ha llegado a colapsar los sistemas administrativos del gobierno de Grecia. Es curioso observar también que, mientras que Estados Unidos y la Unión Europea se disputan el número de autorías de virus casi por igual -con Sudamérica y Europa del Este a los talones-, un gran número de las infecciones que se registran cada año tienen su origen a lo largo de todo el continente asiático con especial intensidad.

El futuro y la evolución son inciertas, aunque lo que parece claro es que los virus tienden a ser cada vez más complejos, debido a las exigencias de la nueva plataforma, y que el camino está abierto hacia la integración con Internet. Los límites están en la propia imaginación de los escritores de virus, y el único freno que existe es el propio tiempo, que es el que va trayendo consigo día a día las innovaciones en el terreno de Win32. La duda está en si las compañías antivirus van a ser capaces de seguir el ritmo frenético de la evolución vírica o si, por el contrario, se verán finalmente desbordadas por la imaginación del lado oscuro de la programación.

Giorgio Talvanti

16/08/1999 Escuchas y censura en Internet

El parlamento de Japón aprobó la semana pasada una polémica ley que da derecho a los policías a interceptar las comunicaciones, como pueden ser las llamadas telefónicas o los emails en Internet. La justificación se enmarca dentro de las necesidades que los agentes tienen para perseguir al crimen organizado.

En realidad se aprobaron tres leyes que tenían como fin la lucha contra el crimen organizado pero, como era de esperar, la polémica saltó en la que daba carta blanca a la interceptación de las comunicaciones.

El gobierno insiste en que esta medida ayudará a los agentes, y que sólo será utilizada en los casos en los que se vean implicados asuntos de drogas, armas, asesinatos y en la entrada de grupos organizados a Japón.

Sin embargo, las explicaciones del gobierno no terminan de convencer a la gran masa social, que ve con miedo la posibilidad de que esta ley dañe los derechos más básicos sobre privacidad e intimidad. A fin de cuentas, se supone que los grupos organizados utilizaran sistemas criptográficos fuera del alcance del gobierno, con lo que para muchos los argumentos esgrimidos son sólo una mala justificación de cara al control de las comunicaciones del ciudadano.

Mientras tanto, en Australia, Internet también se encuentra en el ojo del huracán de la clase política. En esta ocasión, dentro de la normativa que rige los servicios de difusión, se está intentando implantar la censura en cuanto a los contenidos accesibles en la Red.

En principio, se quiere hacer hincapié en el material pornográfico y el clasificado de alto riesgo, como puede ser la construcción de bombas. El gobierno se escuda en que las medidas han sido fruto de la petición popular, donde los padres han ejercido mucha presión preocupados por los contenidos nocivos que sus hijos pueden encontrar en la Red.

De nuevo todo parece indicar que el perjudicado será el ciudadano de a pie, ya que las medidas a tomar no impedirán a las personas con los medios o conocimientos necesarios saltarse este tipo de censuras y seguir accediendo a todos los contenidos. Por otro lado, ya existe en el mercado software de control parental, destinado a restringir contenidos clasificados a los más pequeños, por lo que de nuevo la argumentación del gobierno parece estar fuera de lugar.

Bernardo Quintero

28/09/1999 Cifrado seguro utilizando una simple baraja de póker

Bruce Schneier ha diseñado un algoritmo de cifrado seguro que emplea únicamente una baraja de póker de 54 cartas. Se trata de un algoritmo de cifrado en ristra o flujo ("stream", en inglés), y ha sido diseñado para que sea sencillo y fácil de realizar a mano, sin apoyo informático. El algoritmo se llama "solitaire" y fue creado para la novela Cryptonomicon, de Neal Stephenson, publicada esta primavera. El algoritmo se basa en mover las cartas del mazo siguiendo una serie de pasos, y combinar sus resultados con el documento a cifrar. La clave está constituida por la disposición inicial de las 54 cartas de la baraja de póker, por lo que su fortaleza aparente es de 54! (54 factorial), aproximadamente 236 bits.

Se dá la curiosa circunstancia de que este algoritmo parece lo bastante seguro como para que sea

considerado como tecnología de doble uso (como las minas o las balas de ametralladora) por parte del gobierno estadounidense. Este hecho podría suponer la ilegalidad de exportar el conocimiento de dicho algoritmo a países extranjeros.

Sin embargo la legislación de EE.UU. protege la libertad de expresión escrita, por lo que se permitiría la exportación sin problemas si el algoritmo se describiese en un libro editado de forma legal, con ISBN, etc. Y eso es precisamente lo que se hace en la novela de Neal Stephenson, en la que “solitaire” aparece como un apéndice.
Parece increíble que un algoritmo criptográfico tan sencillo, que puede memorizarse y utilizarse de forma manual, pueda estar sujeto a legislación militar. Pero la legislación norteamericana es así. En cualquier caso Bruce Schneier ha tomado la iniciativa y ha decidido publicar una página web en la que describe con todo detalle el algoritmo, proporciona ejemplos, consejos de uso, código fuente para los que deseen utilizarlo con un ordenador y vectores de prueba para comprobar que las implementaciones son correctas.

El documento original está escrito en inglés, pero Jesús Cea Avión se ha encargado de traducirlo al castellano y hablar con Bruce Schenier para que añada enlaces a la traducción. En este momento, además de la versión en inglés y la versión en castellano recientemente traducida, existen también traducciones oficiales el francés y al alemán.

Jesús Cea Avión

Entrevista



Mercé Molist Ferrer

Mercé Molist Ferrer es periodista freelance especializada en Internet. Ha escrito sobre la red en diversos medios desde 1995. Actualmente colabora en los suplementos “Ciberpaís” y “El País Semanal”, (ambos del diario “El País”) las revistas “@rroba” y “Popular Science”, mantiene el blog Port666, imparte charlas y acaba de poner en marcha el wiki Hack Story, sobre la historia de la cultura hacker.
Fue la primera periodista en hacer referencia a Hispasec en un medio de nivel nacional, y actualmente nos sigue contactando cuando lo necesita. Es probablemente la periodista más veterana, conocida, respetada e involucrada con la red en España.

Hispasec: Una reflexión sobre la seguridad en Internet desde 1998...

Merce Molist Ferrer: Miro los artículos que escribí aquel año y me doy cuenta de que en esencia no ha cambiado mucho. Entonces escribía sobre virus, spam, pérdida de privacidad, cons de hackers (aquel año fui al Chaos Communication Congress y al hackmeeting italiano, que era la primera vez que se hacía). Y también aquel año tuvimos el juicio a !Hispahack. Ahora tenemos virus, spam, pérdida de privacidad, cons y, en vez de persecución a hackers, persecución a gente relacionada con el P2P (que algunos son los hackers de entonces). Así que... poco ha cambiado a grandes rasgos. Se sigue investigando y rompiendo lo que se puede (ahora hay más cosas para romper), el sistema sigue sin entender nada y el usuario sigue siendo igual de ignorante en temas de seguridad, solo que ahora hay más usuarios y les imponen por decreto unos programas (antivirus, cortafuegos) que no saben usar.

¿Qué ha cambiado? Que muchos hackers que conocí entonces ahora trabajan como consultores de seguridad. Que la actividad criminal ha pasado de 1 a 100. Que en vez de meterte un virus tonto ahora te

roban dinero o datos personales. Que empresas y gobiernos están (o lo parecen) mas concienciados por el tema seguridad. Que las empresas de seguridad venden más motos. Que todo se ha hecho bastante más comercial, en ambos bandos.... Y que cansada de la inseguridad de Windows me he pasado a Linux.

En lo que a mi trabajo como periodista se refiere, el cambio más importante es que hay menos información buena sobre seguridad. Quiero decir: ha aumentado muchísimo la información en Internet sobre seguridad, es impresionante, no doy abasto con los RSS, pero es... insípida. No son fuentes directas, no vienen del hacker, de su web, de su ezine, sino que mayoritariamente vienen de las empresas o de intereses diversos. Se ha caído en lo mismo que vemos en los telediarios: que todos dan las mismas noticias, la mayoría incorrectas y salidas de intereses oscuros.

Y, sobre todo, sobre todo, ha desaparecido el humor, la idea del juego que impregnaba los asaltos, los descubrimientos, la forma de contarlos... Ahora todos somos profesionales, los de antes y los de ahora, se perdió por el camino buena parte de la creatividad, del arte... y, con ellos, la gran mayoría de grupos hacker, de aquí y de fuera.

Pero advierto que es una visión subjetiva. Ahora tengo la sensación de haberlo visto todo y, en cambio, en el 98 me lo estaba pasando pipa. Hacía algunos años que escribía sobre Internet y sentía mucha curiosidad por la comunidad y su underground, a los que había dedicado diversos artículos. Era mi forma de aprender: escribir un articulo, que requería que me documentase-estudiase, y así cada reportaje era como hacer un master.

Entonces, El Pais abrió el suplemento Ciberpais, en el 98, y me pidieron que escribiese para ellos y que me encargase de los temas de seguridad y hacking. Así, lo que hasta entonces era simple curiosidad pasó a ser trabajo pagado. ¿Que más podía pedir? Y pude dedicarme a saciar esta curiosidad con una buena excusa. Entonces fue cuando me puse a "estudiar" seguridad más a fondo que antes. ¿Cómo? Leyendo todos los numeros de SET y otros ezines, aprendiendo hasta altas horas de la noche qué era aquello del "spoofing" y de los envenenamientos y el buffer overflow y otros esoterismos para una persona de letras. Mandé un mail de presentación a todos los grupos hacker hispanos que conocía, ofreciéndome a escribir artículos sobre sus logros, y algunos me respondieron y otros me ignoraron. Y, en general, fue una época altamente excitante, de aprendizaje, de leerme entero el Jargon File y otros libros electrónicos sobre el underground de aquí y de fuera (aún los tengo impresos), "SnowCrash" en ingles, que te juro que no entiendes nada, y otros sobre hacking, virus, el "Hackers, heroes of the computer revolution"...

Conocí a gente flipante. Aprendí cosas sorprendentes. Todo era información nueva y genial. Se me abrió la mente como jamás, aquello era "food for thought" en estado puro. Interioricé hasta el fondo de mi corazón esta actitud, esa comunidad, esa diversión y curiosidad intelectual. ¿Cómo, dime, cómo puedo pensar que lo que ha venido después sea mejor? Pero es subjetivo, ya digo, porque para alguien que este aprendiendo ahora, estos son los "exciting days" :).

H: ¿Cuál y cómo fue tu primer contacto con Hispasec?

MMF: Conocía a algunas personas de Hispasec antes de que se crease la empresa. Sé que primero fue "Una-al-dia" y que me suscribí desde bastante pronto, pero no recuerdo los detalles.

H: ¿Estás suscrita a una-al-día? ¿Las lees?

MMF: Si, estoy suscrita. Y sí, al menos el titular me lo miro. Si me interesa, leo el articulo. Y si me interesa mucho, más de una vez he decidido escribir yo misma un articulo sobre este tema, contactando con su

autor en una-al-día y pidiéndole mas información.

H: ¿Cuántas entrevistas has hecho? ¿Quién te ha impactado más de todas tus entrevistas?

MMF: No tengo ni idea de cuántas entrevistas he hecho en mi vida. La que me impactó más no tiene nada que ver con Internet y hace tantos años que está perdida, no existe en formato digital. Era una entrevista a un antropólogo que explicaba sus experiencias con unos indios del Amazonas, su forma de vivir, su filosofía, me impactaron. En cuanto a entrevistas relacionadas con Internet... muchas. Me gusta hablar con personas que tengan puntos de vista abiertos, alternativos, que te puedan sorprender con una idea inesperada, que vibren en tu misma sintonía y que sean auténticos maestros. En este sentido, destacan Wau Holland, me encantaba hablar con él, mucho, Ricardo Domínguez y Richard Stallman.

H: ¿Cuál es el sitio más interesante en el que has estado por trabajo?

MMF: Los hackmeetings italianos. Allí descubrí, en vivo, lo que era el sentimiento de comunidad.

H: ¿Piensas que se ha perdido el "romanticismo" de aquellos primeros días en la red?

MMF: Sí. En aquellos días (yo no estoy desde los primeros, ni mucho menos), quien estaba en Internet era porque era alguien genial, avispado, inteligente. En resumen: "raro". Daba la sensación de que todos los parias del primer mundo estaban en la red. Parias en el sentido de incomprendidos por la sociedad, especialmente por sus geniales mentes y visiones del mundo. Entonces, la red era un reflejo de esas mentes pioneras y, claro, había una calidad flipante.

H: ¿Cómo y por qué te metiste en esto?

MMF: Por curiosidad. Trabajaba como "freelance" y estaba suscrita a la revista "Newsweek", para ver por dónde iba el mundo y, si acaso, sacar ideas para reportajes. Vi que hablaban todo el día de una cosa llamada Internet, de la que no se hablaba en España. Puse la antena e investigué cómo entrar. Entonces colaboraba en "La Vanguardia" y me las apañé para poder ir un día a la semana y usar su Internet, básicamente la web, para sacar documentación para reportajes. El único proveedor en España entonces era Goya y sus precios era prohibitivos para mí. Cuando abrió Servicom, en el 95, me apunté. Fue una odisea, para alguien que no tenía amigos informáticos y solo sabía usar el Wordperfect y cuatro cosas de MS-DOS. Aun hoy no entiendo cómo conseguí yo sola hacer funcionar aquel módem. Debían ser enormes mis ganas :).

H: ¿Por dónde andarán los tiros en seguridad en el futuro?

MMF: Se normalizará. Sera como hoy en el mundo real. Hay inseguridad, se maneja fatal, está todo el sistema mal montado, las cárceles no sirven, la policía tampoco, funciona fatal, pero se va tirando. Por una parte, porque hay cierto orden dentro de lo que es la inseguridad y, por otra parte, porque nos hemos acostumbrado y no nos llevamos las manos a la cabeza por cosas que quizá nuestros abuelos sí se llevaban las manos a la cabeza. Se normalizará. A costa de un control férreo y de la pérdida de muchos derechos, eso también hay que decirlo. 1984 era un juego ante lo que viene.

H: ¿A qué dedicas más tiempo últimamente?

MMF: A las cosas de fuera de la red que olvidé cuando estaba obsesionada con ella, empezando por mí misma. Y, dentro de la red, hace poco he encontrado un nuevo juego que me tiene abducida: montar un wiki con la historia de la comunidad hacker española. La razón es la siguiente: un día, mirando las pocas historias de la Internet española que se han escrito, me di cuenta de que la gente que yo conocí, los

auténticos hackers, los que de verdad construyeron la red, no salían. Solo se mencionaba a señores con corbata, instituciones y empresas especialistas en colgarse medallas.

Si alguien no lo explica, las generaciones futuras creerán que, realmente, esa gente inventó nuestra red y el recuerdo de aquellos hackers desaparecerá para siempre. Llámame justiciera :).



Primera referencia a Hispasec a nivel nacional



EL PAÍS, jueves 4 de febrero de 1999

ciberp@is 13

PORTALES

Yahoo! reúne con la compra de Geocities al 60% de los internautas

Compaq, fabricante de ordenadores, decide sacar a bolsa el buscador Altavista-Magallanes

Javier Martín

Yang y Filo compran barato. Falta saber si compran bien.

Mientras la mayoría de los portales se unen a sociedades que les aportan tecnología de primera línea, los fundadores de Yahoo se han gastado 670.000 milllones de pesetas en comprar Geocities, la primera comunidad virtual, con 11 millones de páginas alojadas por sus 3,5 millones de miembros activos. Yahoo y Geocities reciben mensualmente la visita de 80 millones de intenautas diferentes.

Yahoo pagará (en acciones) por Geocities 670.000 millones de pesetas. La pasada semana, ATHome había pagado por el portal Excite una cantidad similar. Este aluvión de compras en los que están implicados portales de Internet está justificando la sobrevaloración de sus acciones. Baste decir que a Ford le ha costado la compra de la Volvo, menos que lo que le costó a AOL adquirir Netscape (un billón de pesetas).

Tras la absorción, Netcenter, el portal de Netscape, ha iniciado una nueva época con nuevos servicios. A la vez, el fundador de Netscape, tras su año sabático, se ha incorporado como jefe de tecnología de AOL. Marc Andreessen, de 27 años de edad, ayudó a inventar el navegador que popularizó Internet.

Andreesen, que con la compra de AOL se embolsó 25.000 millones de pesetas, es una figura clave para que una compañía como AOL, dedicada a proporcionar servicios personales, tenga un respaldo tecnológico de primera línea, algo de lo que siempre se le ha acusado que carecía.

El cambio estratégico de los portales, que han pasado de proporcionar servicios al internauta a proporcionar los servicios [illegible] del internauta, hace [illegible] detrás una tecnología de primer orden para que no se quede como un mero alamcén de *webs*.

En ese sentido se movió AtHome, una empresa de cable, cuando compró el portal [illegible] AOL anunció que ellos contratarían con la Bell Atlantic un servicio de DSL para sus 15 millones de abonados.

Además el portal Snap! (creado por la revista electrónica CNet y comprado por la NBC) anunció su producto Cyclone para dar la máxima velocidad y potencia a su portal.

Jeff Mallet, presidente de Yahoo, no cree, por el momento, en el cable ni siquiera quiere hablar de ningún acuerdo preferencial con compañía telefónica [illegible]. La estrategia de sus fundadores [illegible] Filo, se dirige a comprar audiencia [illegible] bles. Yahoo cuenta con el respaldo económico (30% de las acciones) del japonés Softbank, que [illegible] intereses en Geocities.

Altavista, a bolsa

En la pelea del portal también participan Go (Walt Disney más Infoseek), Snap!, MSN (Microsoft) y Lycos.

En la mediación de audiencias de diciembre, realizada por Mediametrix, aol.com obtuvo 49,8 millones de usuarios diferentes; seguido de yahoo.com, con 47,3; geocities.com, 33,4; msn.com, 32,9; netscape.com, 30,9; excite.com, 25,3; lycos.com, 23,2; microsoft.com, 22,9; bluemountanrts, 21,7; Infoseek.com, 21.1, Altavista, 19,8.

Precisamente Compaq, dueña de Altavista, ha anunciado que [illegible] bolsa a este buscador-portal, para [illegible] compañía aparte. Sin embargo para el presidente de Yahoo! Mallet, sus futuros competidores serán AOL y el msn de Microsoft. De momento, Yahoo! les lleva un largo de ventaja, exactamente el 60% de los usuarios de la red.

Jerry Yang, cofundador de Yahoo!, en su visita a Barcelona hace tres años. / ANTONIO ESPEJO

AUDIENCIAS: [illegible]
YAHOO: [illegible]
GEOCITIES: www.geocities.com
EXCITE: www.excite.com
ALTAVISTA: www.altavista.com

El sitio español HispaSec se dedica a dar servicios sobre problemas de **seguridad** informática

Mercè Molist

Justo cuando moría 1998, se abría en la Red el primer servicio de información en español sobre seguridad informática: HispaSec. Desde entonces y sin funcionar aún a pleno rendimiento, ha conseguido un notable éxito, que se explica por la solidez del proyecto, apadrinado por algunos de los más reputados expertos del país, como Jordi Murgó o Jesús Cea, y su originalidad, ya que no existía nada semejante en la Internet hispana.

La espina dorsal de HispaSec es *Una al día*, un servicio diario de envío, por correo electrónico y previa suscripción gratuita, de noticias sobre seguridad, desde virus y parches de programas hasta criptología o *hardware*. Desde octubre ha estado funcionando en prueba.

"*Una al día* nació de forma espontánea en una lista de distribución de técnicos de revistas especializadas en informática", explica Bernardo Quintero, artífice del invento junto a Antonio Ropero. "El desencadenante fue la queja por parte de uno de ellos por la escasez de noticias que generaba la seguridad informática. Ante este comentario, que no compartía, afirmé que sería capaz de enviarles todos los días una noticia sobre seguridad. Tras las primeras semanas, empezaron a llegarnos solicitudes de entrada de especialistas de seguridad informática y comenzamos a darnos cuenta de la repercusión que podía tener la iniciativa".

Las noticias diarias aparecen también y quedan archivadas en el sitio, ordenadas por temas y acompañadas de otros artículos más profundos sobre nuevos métodos criptológicos, análisis de virus, seguridad en redes, etc.

Además, está en pruebas un servidor de llaves PGP y se espera poner pronto en marcha nuevas secciones, entre las que destaca *H-BaSec* que quiere ser, según Ropero, "la más completa base de datos de vulnerabilidades y parches en español".

Otro proyecto es la creación del, según Quintero, "detector de antivirus más potente del mundo: unir a los mejores antivirus en nuestro servidor, de manera que un usuario, a través de Internet, pueda dejar un fichero que crea infectado y se le dé el resultado en línea, con la potencia de todos los antivirus".

Página de HispaSec.

HISPASEC: www.hispasec.com

TELENEGOCIOS

El portal de 'Latinred'

La empresa creadora de Latin Mail y Latin Chat utilizará la marca Latinred.net para su nuevo portal, en el que incluirá, además de servicio de correo gratuito y tertulia, los servicios clasificados, postales y fútbol que hoy tienen dominio propio: *www.usados.net*, *postales.latinmail.com* y *www.futbolmania.com*.

Traductor en la red

El nuevo producto de la red Intelinet (*www.mte.intell.net.mx*), de México, es el traductor de páginas web en la red que no requiere instalar ningún programa extra. El traductor es gratuito e interactivo y la información para activarlo se encuentra en *www.mte.intell.net.mx/tradu*.

'Bilbaoweb.com'

Bilbao es una ciudad realmente virtual (*www.bilbaoweb.com*), en la que pueden verse imágenes de sus distintos barrios, además de información práctica.

Música música.

Para profesionales de la música

Bemar Net Management, empresa de la localidad valenciana de L'Eliana, ha adquirido *www.musices.com*. Este sitio se ha desarrollado en torno a un sistema de bases de datos que contiene cerca de 5.000 registros relacionados directamente con la música, agencias de espectáculos, arreglistas, conservatorios, escuelas de música, discográficas, emisoras de radio, promotores, escenarios, etcétera.

Premio al sitio de Audi TT

El sitio español de Audi TT (*audi.vw-audi.es/tt*), realizado por la agencia interactiva Double You, ha sido premiado en el [illegible] de comunicación interactiva por la revista [illegible] Communication Arts (*www.commarts.com* [illegible] *dex.html*), dedicada al diseño y la creatividad. Se trata del primer sitio web español que premia esta revista.

Postaweb en italiano.

Mix Mail se abre a Europa

La empresa 100% Net Partnership, creadora del correo electrónico gratuito basado en la web llamado Mix Mail, ha anunciado que su base de datos alcanza los 300.000 usuarios registrados y ha lanzado su versión Italiana, localizable en *www.postaweb.com*, con lo que inicia así su expansión europea.

Mixmail no requiere ningún otro *software* adicional al navegador. Esto significa que los usuarios pueden utilizar con seguridad sus cuentas personales de [illegible] electrónico desde cualquier [illegible] del mundo conectado a [illegible].

Comp[illegible] dominio gratis

[illegible] *Domain.com* permite comprobar gratuitamente si el dominio que se desea registrar aún está disponible.

Capítulo

2

7C0

3720

AÑO 2000

11111010000



946684800 – 978307199

Durante este año...



_ En enero, **AOL (America On-Line)** anuncia un acuerdo para comprar la empresa Time Warner por 162.000 millones de dólares. Resulta en la fusión de empresas más grandes del mundo, creando todo un imperio.

_ Después de “Volver a empezar” de José Luís Garci en 1983, y “Belle Epoque” de Fernando Trueba en 1994, Pedro Almodóvar recibe el Oscar a la mejor película de habla no inglesa con **“Todo sobre mi madre”**, recogiendo el premio de manos de Penélope Cruz y Antonio Banderas después de un escandaloso grito.

_ En marzo, el Ministerio de Sanidad permite a los científicos realizar **experimentos genéticos** en pacientes.

_ En la una-al-día del 23 de marzo, “¿Qué son los “hypes” y cómo nos afectan?” Giorgio Talvanti escribe “Como no podría ser de otra manera, el que suscribe se centra una vez más en su especialidad, el campo de los virus informáticos y demás especímenes agrupables bajo el hiperónimo de **“malware”**. Usando por primera vez esta última palabra.

_ El Partido Popular alcanza mayoría absoluta en las elecciones legislativas de marzo, dejando muy atrás al candidato del PSOE Joaquín Almunia. **José María Aznar** renueva así su mandato cuatro años.

_ En noviembre de 1999 **Elián Gonzáles** de 6 años huye de Cuba hacia Estados Unidos. En el trayecto realizado con una barcaza muere (entre otros) la madre. Los supervivientes alcanzan las costas de Florida después de varios días a la deriva. El pequeño es rescatado por dos pescadores y entregado al servicio de Guardacostas de los Estados Unidos. Según las leyes de Estados Unidos, la madre de Elián cometió un secuestro. Sin embargo, dada la práctica jurisprudencial estadounidense “wet feet, dry feet”, los cubanos que alcanzan las costas de los Estados Unidos pueden solicitar asilo político. Los que son hallados en el mar son devueltos a Cuba. Comienza un importante conflicto diplomático entre ambos países con un niño de 6 años como protagonista. La fiscal general de Estados Unidos, Janet Reno, pone fecha límite el 13 de abril para devolver al crío. Empieza el pulso. El 22 de abril de 2000 el Departamento de Justicia ordena que Elián sea sacado por la fuerza de la casa de Florida en que se encuentra y entregado a su padre. En una exagerada puesta en escena, un numeroso grupo de agentes del INS (Servicio de Inmigración y Naturalización) vistiendo uniformes de combate y armados de subfusiles automáticos toman la casa donde se aloja Elián. Una fotografía célebre de Alan Diaz de Associated Press (que le proporcionaría el Premio Pulitzer en 2001) muestra a un agente del INS apuntando con el dedo fuera del gatillo a Elián. La fotografía daría la vuelta al mundo.



_ En abril el estado de Vermont en Estados Unidos, legaliza la unión civil entre **parejas del mismo sexo**.

_ Sony pone a la venta la **Playstation 2**. Es la consola más rápidamente vendida de la historia y con la perspectiva del tiempo, la que más ha perdurado. 8 años después de su lanzamiento, todavía es posible adquirirla original en tiendas y se siguen creando juegos en exclusiva para esta exitosa versión de Sony, que obligaría a retrasar su Playstation 3 hasta 2007. Ha

vendido más de 100 millones de unidades. Su primera versión tenía una CPU de 294 Mhz y 32 megas de RAM. Cuesta unos 300 dólares.

_ **"405"** es el primer corto distribuido ampliamente por Internet. Se trata de una de las primeras campañas que se beneficia del efecto de márketing viral en la Red. Tiene más de dos millones de visitas en un mes. Costó 300 dólares y 3 meses de realización. Logra una gran repercusión mediática en Estados Unidos.

_ Se lanza el **Pentium 4**, cuya producción continúa en forma de varios núcleos hoy en día. En agosto de 2000 se llega a los 2 GHz de velocidad. Sufre muchos problemas con sus primeros modelos (no llegarían a su completa madurez hasta 2004) y muestran rendimientos inferiores a los Pentium III y a su principal competidor del momento, la línea Thunderbird de AMD. Comercialmente, Intel decide romper con la numeración romana que había adoptado hasta el Pentium III. Considera que no sería entendida por todo el mundo.

_ En el año 2000 entra en funcionamiento la primera plataforma comercial de Televisión Digital Terrestre (TDT) en España, **Quiero TV**. No alcanzaría la rentabilidad esperada y cesaría sus emisiones el 30 de junio de 2002.

_ En la una-al-día del 28 de julio, "Hispasec y una-al-día accesibles vía WAP" se añade el enlace **"opina sobre esta noticia"** por primera vez, con comentarios públicos.

_ **Google** firma un acuerdo con Yahoo!, buscador líder del momento. En los resultados de Yahoo! Se puede observar la leyenda "powered by google" y la explosión de Google comienza. Los usuarios acceden a google.com y se sorprenden por la sencillez y limpieza de una página diseñada exclusivamente para buscar. La web de Yahoo! por el contrario se encuentra artificialmente recargada con decenas de servicios, y el buscador es sólo una pequeña caja en la parte superior. Además de esta ventaja, los internautas agradecen que con este nuevo buscador los resultados no están adulterados por ningún tipo de publicidad. Se corre la voz y su popularidad se multiplica.

En agosto se hunde el **submarino ruso Kursk** en el mar de Barents. Una serie de desgracias ocurren en cadena a causa del derrame de una sustancia química. Explotan varios torpedos y el submarino se hunde hasta el fondo del mar. Se intenta silenciar la tragedia, pero sale a la luz. Varias naciones prestan ayuda para un rescate agónico y complicado. Se filtra información contradictoria sobre si existen supervivientes o no. Más tarde, las notas dejadas por los tripulantes que sobrevivieron las primeras horas de hundimiento y explosiones, demostrarían que al menos 16 de los tripulantes se refugiaron durante seis días en partes estancas traseras tras las explosiones. Pero el daño en el casco estaba hecho y a medida que el agua subía, un incendio se declaró en el interior y murieron asfixiados. Al rescatar el submarino se recuperan 3 notas de los supervivientes, solo 2 son hechas públicas y no en su totalidad.

_ En septiembre se inauguran los **Juegos Olímpicos de la XXVII edición en Sydney**. España consigue 11 medallas.

_ En noviembe, el gobierno de **Saddam Husein** rechaza las nuevas propuestas del Consejo de Seguridad de la ONU para realizar más inspecciones en busca de armas de destrucción masiva. Este tema retomaría fuerza en 2003 y terminaría declarándose la guerra.

_ Bajo la eterna sospecha de fraude e irregularidades (en parte por las famosas tarjetas “mariposa”), el candidato republicano **George W. Bush** derrota al vicepresidente demócrata de la era Clinton, Al Gore. Se vive un agónico recuento de los votos en el estado de Florida durante un mes.

_ A final del 2000 se presenta la **versión 6.0 de Netscape Navigator** tras dos años de desarrollo, basándose en el navegador Mozilla. A mediados de año Netscape pierde fuelle ante la imparable escalada de Internet Explorer. 86% de uso frente a un 13% que nunca remontaría.

Seguridad Informática



_ En enero se publica **SubSeven 2.1 Gold**, que junto a BackOrifice y NetBus son sin duda los troyanos (defendidos como herramientas de administración remota) clásicos más conocidos del momento. Como otros troyanos similares consta de dos partes, la que se instala en el ordenador atacado hace las veces de servidor, mientras que la parte que emplea el atacante es el cliente. Esta versión de SubSeven incluye nuevas características como libro de direcciones, visor de procesos, explorador de IPs remotas, webcam, texto a voz, espías de ICQ, Microsoft Messenger y Yahoo Messenger, visor de portapapeles, movimiento del ratón remoto, abrir y cerrar la unidad del CD-ROM, control del sistema de archivos y un largo etcétera de posibilidades.

_ Según fuentes gubernamentales chinas, cualquier compañía que se implante dentro de su república deberá poner a disposición de técnicos de su gobierno el **código fuente de los programas** que se utilicen para transmitir información de forma cifrada.

Las redes globales de espionaje se ponen de moda. La NSA, Agencia estadounidense para la Seguridad Nacional, desclasifica unos documentos, secretos hasta ese momento, que confirman el nacimiento del mayor programa de espionaje conocido hasta la fecha. Este megaproyecto apodado **Echelon** consiste en una red de ámbito internacional dedicada a la interceptación indiscriminada de todo tipo de comunicación electrónica: telefonía, fax, Internet, etc, gracias al conglomerado de satélites y sistemas informáticos sustentados por los servicios secretos de países como EE.UU, Gran Bretaña y Canadá. Quedan bajo su dominio tanto usuarios individuales como corporaciones y estamentos gubernamentales. Gran parte de su despliegue a escala mundial toma como receptores de estas escuchas las bases que Estados Unidos mantiene en los países que componen Echelon. Estos datos son enviados posteriormente a la central de la NSA para su análisis. Además del supuesto fin militar, todo parece indicar que el espionaje también es aprovechado con fines puramente económicos. El gobierno francés dice que demandará a los gobiernos de Estados Unidos y Reino Unido por ello, tras hacer público que han estado espiando las comunicaciones francesas durante décadas. Dicen, por ejemplo, poseer pruebas de que la pérdida de un contrato de 3.5 miles de millones de libras esterlinas del consorcio europeo Airbus en 1995 en favor de la compañía norteamericana Boeing, fue debido al espionaje de su oferta.

El servicio secreto ruso, heredero de la antigua KGB, toma posiciones dentro de los ISPs rusos y obliga a mas de 350 servidores de Internet de este país a implantar un software para el **control de las comunicaciones**. La creación de este departamento dentro de los servicios de seguridad rusos denominado SORM-2, nace con la misma excusa que Echelon de controlar las comunicaciones de terroristas y grupos organizados que utilizan Internet

para comunicarse entre ellos. En una carta remitida por Londres a sus socios europeos como contestación a la denuncia realizada por la Comisión Europea, después de salir a la luz la posible colaboración por parte de los británicos con la red Echelon, Inglaterra manifiesta no haber realizado ninguna escucha aunque se siente con todo el derecho a realizar tareas de espionaje sobre el resto de Europa. El Gobierno Británico se ampara en una ley del año 1985 por la que faculta a sus servicios secretos para poder interceptar todo tipo de comunicaciones para salvaguardar la seguridad nacional y hacer prevalecer el bienestar económico entre sus ciudadanos. La fantasía entorno a una gigantesca red de espionaje se dispara. EL parlamento europeo crearía un informe publicado en 2001 en el que se concluye: "las capacidades técnicas del proyecto probablemente no iban tan lejos como han asumido algunos medios de comunicación".

_ En febrero un investigador de la Universidad Autónoma de Barcelona, Andreu Riera Jorba, propone soluciones para muchos de los problemas tradicionales del **voto electrónico**. Años después todavía no se ha aceptado como forma fiable de votación.

_ **Juan Carlos García Cuartango** descubre una puerta trasera en Internet Explorer por la que Microsoft podría instalar cualquier aplicación sin permiso ni conocimiento de los usuarios. Ofrece una página web que lo demuestra. Él mismo explica: "El componente Active Setup requiere software firmado para actuar, el truco de Microsoft es que el software firmado por ellos se instala sin ningún tipo de aviso al usuario (al contrario de lo que ocurre con el resto de casas) y sin necesidad de que se encuentre en la lista de certificados y compañías en los que se confía".

_ Es el año de los problemas de las páginas dinámicas en PHP, ASP y los CGI. Un gran error por parte de **Telefónica** permite que los datos de las facturas de cualquier abonado de Telefónica (lo que incluye nombre, dirección, NIF, e incluso cuenta bancaria y desglose de llamadas) queden accesibles a la consulta de un navegador. El problema proviene de un fallo de programación y configuración del servidor web. Lo arregla en tiempo récord. Cibertienda, el paquete de **Banesto** para la implantación de tiendas virtuales, se ve aquejado de un fallo que puede permitir a cualquier visitante de una de las tiendas alterar el contenido de los carritos de la compra de otros clientes.

_ El 2000 es un año bisiesto. Muchos programas cometían el error de considerar el **2000 como año no bisiesto**, al tratarse de un múltiplo de 100, ignorando la regla de los múltiplos de 400 que sí son bisiestos. Gran número de sistemas se ven afectados por el problema del 29 de febrero. Japón reconoce fallos en registradoras, sistemas de predicción meteorológica y sísmica e incluso una planta nuclear.

_ Microsoft lanza en febrero **Windows 2000**, y comienza la era NT 5.0. El sistema operativo tiene una gran aceptación, supone un paso adelante en tecnología y fiabilidad para Microsoft. Aunque no tenía en cuenta la seguridad por defecto, con el Service Pack 4 y una buena configuración manual, Windows 2000 resultó un gran producto que todavía es muy usado, casi 9 años después de su lanzamiento. Ese mismo año, en julio, sacaría su primer Service Pack.

_ En marzo Microsoft soluciona el problema del bloqueo al ejecutar en una consola el comando **con\con**, 15 días después de advertir sobre el problema.

_ Siguen los problemas de privacidad. Salta a todos los medios el caso de **Advert.dll**, una librería que se instala con un gran número de aplicaciones shareware de renombre, y que según todas las informaciones está destinada a espiar las transmisiones de los usuarios.

_ Nace **CriptoRed, la Red Iberoamericana de Criptografía**. Se presenta como uno de los proyectos más ambiciosos dentro del campo de la difusión criptográfica a través de Internet. Esta red de cooperación docente con todos los países de Iberoamérica, cuenta en solo 3 meses con más de 100 miembros, la mayoría de ellos profesores de reconocido prestigio académico e investigador, así como buen número de universidades y centros de investigación. Hoy en día continúan sus actividades con éxito.

Es el año del virus **LoveLetter**. Aparece en mayo. Se trata de código Visual Basic Script y se envía principalmente a través del correo electrónico y el IRC. Consiste en un mensaje con el asunto "ILOVEYOU" y el fichero adjunto LOVE-LETTER-FOR-YOU.TXT.vbs. La extensión VBS (Visual Basic Script) puede permanecer oculta en las configuraciones por defecto de Windows, lo que hace pensar que se trata de un inocente archivo de texto. Cuando se abre el archivo el gusano infecta el sistema y se expande rápidamente enviándose a los contactos en la agenda del Outlook, incluidas las agendas globales corporativas. Rápidamente se convierte en un fenómeno mediático.

Según las primeras líneas de código el gusano procede de Manila, Filipinas, y el autor se apoda "spyder":



rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group / Manila,Philippines

Este gusano obligaría a Microsoft a publicar poco después una actualización de funcionalidades de seguridad para su Outlook. La actualización (Outlook 98/2000 e-mail security update) aporta varias características. Impide la ejecución directa de un buen número de extensiones e incorpora dos zonas de seguridad a Outlook. Bajo la zona 1 se incluirán 28 tipos de archivos con las extensiones potencialmente peligrosas más conocidas.

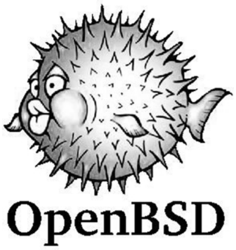
_ Hispasec publica su **comparativa antivirus 2000**, tras el éxito de la comparativa de 1999, que revolucionó toda la metodología de pruebas antivirus a nivel mundial hasta el momento. Ese año se sigue innovando y se presenta la mayor comparativa antivirus de la historia, analizando un total de 30 productos seleccionados entre los mejores de todo el mundo. Una de las pruebas (hasta el momento sólo realizada por Hispasec) consiste en el envío de una muestra de virus real, pero no detectado por ningún antivirus, para comprobar la velocidad de respuesta y efectividad de los servicios técnicos de cada firma.

_ En junio, se sabe que un juego de Disney Interactive, distribuido en España por Infogrames, lleva en su interior el **virus CIH activado**, uno de los más dañinos de toda la historia. Una "sorpresa" que ambas compañías intentan silenciar. Concretamente el archivo "RT4.EXE", perteneciente al juego "El Reino de las Matemáticas con Aladdin" se ve afectado. El desconcierto surge cuando ningún antivirus detecta presencia alguna del virus en el CD original de instalación.

_ Los gusanos programados en Visual Basic Script (VBS) están de moda. Tras la fulgurante irrupción de "I love you" y todas sus mutaciones, se detecta un malware de menos de 12 kilobytes de longitud, **"Timofónica"** creado en España. Programado en VBS es capaz de autoenviar copias por medio de correo electrónico a todas las cuentas almacenadas en la libreta de direcciones del usuario además de mandar mensajes cortos a teléfonos móviles escogidos al azar. También instala un troyano que, al siguiente

arranque, borra los datos de la CMOS y formatea el disco duro de tal manera que no se pueden recuperar los datos perdidos por medio de ninguna aplicación específica.

_ Tras observar los buenos resultados con respecto a la seguridad que ofrecía la configuración por defecto del sistema operativo **OpenBSD**, los orgullosos desarrolladores establecen como lema de su página el logro que estaban consiguiendo. A mediados de 2000, se pueden leer las frases: “Tres años sin un agujero remoto en la instalación por defecto” y “Dos años sin agujero local en la instalación por defecto” junto con el pez globo que representa este sistema operativo. Esta última afirmación sobre la seguridad en local duraría poco, y para finales de ese mismo año 2000 la sentencia ya había sido retirada. En junio de 2002, cuando la frase ya hablaba de “seis años sin agujeros remotos”, el eslogan tendría que ser modificado de nuevo. Se encontraría un grave fallo de seguridad en OpenSSH que permitía a un atacante remoto obtener total control del sistema. Desde entonces hasta 2007, se podría leer “sólo un agujero de seguridad en la instalación por defecto en más de 10 años”.



_ **P3P (Platform for Privacy Preferences Project)**, desarrollado por el World Wide Web Consortium, se presenta como una ayuda para mejorar la privacidad de los usuarios en la web. Pretende estandarizar la industria del sector y automatizar la vía para que los usuarios tengan el control sobre sus datos personales o la información que recogen las webs visitadas. El control se realizaría mediante un formulario, que sería a la vez fuente de información y límite para las webs visitadas. Se supone que las páginas no podrán almacenar dicha información en formato legible y se supone que otros navegadores y usuarios no podrán acceder a esa información personal. Para defensores del proyecto P3P, este método impulsaría a los usuarios a controlar sus propias políticas de privacidad de datos, mediante un formulario sencillo de entender. Fracasaría estrepitosamente.

_ Se crea **“Búfer abierto”**, una nueva sección en Hispasec en la que tendrán cabida las contribuciones que los lectores de Hispasec hagan llegar, a través de la dirección bufer@hispasec.com a modo de noticias y artículos. Siempre con el tema de la seguridad informática como telón de fondo, “Búfer abierto” brinda la oportunidad a los usuarios de Hispasec de publicar cualquier contenido que quieran compartir con el resto de la comunidad. La propuesta no tendría mucho éxito.



_ El concurso televisivo **Gran Hermano** consigue superar todos los récords de audiencia en España, se convierte en verdadero fenómeno social. Se publican en una página web todos los datos de las personas que se presentaron a las pruebas de selección. Alguien entra en los servidores y hace pública la información. Según comprueba Hispasec, Zeppelin TV, la productora del concurso, presenta además un gran número de vulnerabilidades en su servidor.

_ Sigue de moda la privacidad y el espionaje global con el reconocimiento de la existencia de **“Carnívoro”** por parte del FBI. Entre algunas de las peculiaridades de Carnívoro se sabe que no es un único software sino que se compone de diferentes programas incluidos en un mismo paquete. “Carnívoro” es la continuación de otro programa desarrollado con la misma finalidad por el FBI denominado “Omnívoro”, este fue creado originalmente a principios del año 1997 para plataformas Sun Solaris x86. Omnívoro queda en el olvido, pero es reemplazado por “Carnívoro”, desarrollado para plataformas NT.

_ Georgi Guninski descubre de nuevo un agujero en un producto de Microsoft. En esta ocasión el problema puede permitir la ejecución arbitraria de código al abrir un documento de **Microsoft Word 2000**. Lamentablemente se descubrirían muchísimos más años después. Especialmente en verano de 2006.

_ Aparece **Sysid**, un espécimen programado en Delphi (de 200 kilobytes tras haber sido procesado por medio del compresor Aspack, reduciendo los casi 400 originales de peso). Muy pesado para la época, aunque hoy en día podemos encontrar malware creado en Delphi de varios megas de peso. La aportación novedosa que efectúa este virus consiste en lo que en virología informática se conoce como desactivación "on the fly": el malware esconde todo indicio de su presencia en cada momento susceptible de poder ser examinado por el usuario o por algún producto antivirus. En el caso de Sysid, el gusano escribe su clave de activación en el registro sólo en el momento en que detecta que la sesión activa de Windows está siendo cerrada, y la borra tan pronto como es ejecutado en el siguiente arranque y su presencia en memoria está ya garantizada. Se asegura de esta forma el no poder ser ni descubierto ni desactivado, a menos que el usuario conozca en detalle las características del malware y elimine los ficheros semilla instalados en los directorios del sistema.

_ La Fundación para la Privacidad (Privacy Foundation) hace público un comunicado donde describe la posibilidad que tienen los documentos de Microsoft Office de permitir a sus autores seguir el rastro de los usuarios que los leen y las organizaciones por las que se transmite. En el aviso de la Privacy Foundation se hace referencia a la posibilidad que tiene Microsoft Word, Excel y PowerPoint de incluir, lo que se da en llamar, **"Web bugs"**. Estos chivatos o espías permiten al autor del documento detectar y rastrear fugas de documentos confidenciales de una compañía, posibles infracciones del copyright de informes y boletines o monitorizar la distribución de notas de prensa.

_ En septiembre, el sitio web de **Western Union** sufre una intrusión. Los atacantes se hacen con la información de 15.700 tarjetas de crédito y débito de usuarios que utilizan sus servicios. La compañía atribuye el agujero de seguridad al error de un administrador del sistema durante unas operaciones rutinarias de mantenimiento. Este patrón de robos a grandes compañías que almacenan datos privados de usuarios no pararía de producirse esporádicamente en los años posteriores.

_ En octubre Erkki Liikanen, comisario de la **comisión europea de Empresa y Sociedad de la Información**, da a conocer los principios en los que se basará la Unión Europea para luchar contra los delitos que se realicen en Internet. El comisario informa de que se potenciará la formación de los usuarios, se incrementarán las medidas de seguridad en la red y se fomentará la cooperación internacional. Para aplicar esta política se tipifican los delitos en dos grandes grupos. En el primero se parte de la base de que los delitos que se cometen fuera de Internet lo son también si se realizan dentro de la red. Separados en un segundo apartado se encuentran los delitos propios de las nuevas tecnologías, como el "cracking" y los virus informáticos.

_ Tras un largo proceso de casi cuatro años, el NIST (Instituto Nacional de Estándares y Tecnología) norteamericano selecciona al algoritmo **Rijndael como estándar AES**. NIST hace público el algoritmo ganador de la convocatoria AES (estándar de cifrado avanzado), que sustituye al DES (estándar de cifrado de datos) hasta bien entrado el siglo 21. Para sorpresa de muchos, Rijndael es un algoritmo belga, venciendo a algoritmos norteamericanos y a criptólogos de reputada fama mundial. Se quedan atrás "twofish", diseñado por un equipo liderado por el conocido Bruce Schneier (autor, entre otras cosas, del libro "Applied Cryptography"), y al algoritmo "RC6", diseñado, entre otros, por Ronald Rivest (la "R" del algoritmo RSA). Se establece que los programas y hardware que incorporen AES podrán ser exportados fuera de EE.UU., lo que incrementará tanto la seguridad como la interoperatividad de los productos con tecnología criptográfica.

_ Una semana después de ser descubierto, Microsoft facilita un parche que elimina una grave vulnerabilidad en su **Máquina Virtual de Java (Microsoft VM)**. El problema que corrige, descubierto por Georgi Guninski permite la ejecución de código arbitrario en los sistemas de los usuarios con tan sólo visitar una página web o leer un mensaje de correo HTML. La máquina virtual de Java de Microsoft dejaría de ser actualizada o incluida en sus productos en 2004 y terminaría definitivamente su soporte en 2008.

_ La utilidad **traceroute**, utilizada por cualquier administrador de redes, contiene una vulnerabilidad que permite que un usuario local obtenga privilegios de administrador o "root". La vulnerabilidad afecta a las versiones anteriores a la "traceroute-1.4a5-16", distribución LBL.

_ Microsoft publica **versiones para entornos Unix de Internet Explorer y Outlook Express**. En concreto para Solaris y HP-UX. Luego Microsoft no proporcionaría actualizaciones de seguridad para estas nuevas versiones. Ni facilitaría para estas plataformas las versión 5.5.

Se publica en octubre una nueva variante de la vulnerabilidad de escalada de directorios en Internet Information Server. Esta vez, saltándose con codificación Unicode la restricción de los caracteres ".." impuesta por el servidor.

```
http://servidor.iis.afectado/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
```

Muchos años después, seguiría siendo la forma más sencilla y predilecta de muchos de burlar la seguridad de servidores web.

_ Comienza noviembre con el **"Caso Microsoft"**. El Wall Street Journal publica que unos atacantes podrían haber accedido al código fuente del software de Microsoft, incluyendo las últimas versiones de Windows y Office. Este mismo diario cita a un familiar de una persona cercana al caso, que filtra el nombre del troyano "Qaz" como posible herramienta para introducirse en la red interna de Microsoft a través de un mensaje de correo electrónico. El troyano, tras ser ejecutado por un empleado de Microsoft, habría abierto una puerta trasera en el ordenador infectado que facilitara el acceso al atacante y la posterior instalación de otras herramientas para conseguir contraseñas y acceso a información sensible. Bernardo Quintero desmonta en una serie de entregas de una-al-día la teoría del troyano Qaz, analizando detenidamente su comportamiento y cómo sería técnicamente inviable que se hubiera usado este programa para vulnerar la red, hipótesis sin embargo avalada por otros "expertos".

_ El CERT norteamericano hace pública su **nueva política a la hora de difundir avisos de seguridad**. En ella se indica que los problemas de seguridad serán anunciados de forma pública a los 45 días del aviso inicial, independientemente de que existan o no soluciones por parte de los fabricantes. El CERT fue creado en 1988 por el gobierno americano, tras el conocido ataque del "gusano de Morris" que contaminó el 10% de todas las máquinas conectadas a Internet.

_ En noviembre se detecta la primera unión estrecha entre **malware y banca online**. Se descubre Req, un gusano que roba información de un banco de Suiza. Una vez ejecutado, el gusano procede a buscar en el disco duro del usuario infectado documentos generados por un programa que el Union Bank de Suiza proporciona a sus clientes para efectuar pagos por medio de Internet (una especie de resguardos electrónicos) y, en caso de encontrar alguno, lo envía a tres direcciones de correo pertenecientes al autor del malware.

_ **Hybris**, un gusano programado por el mismo autor que Babylonia, se presenta como el malware más difícil de combatir. Probablemente, también el más complejo aparecido hasta el momento.

_ A final de año, fruto de la colaboración tecnológica entre **Hispasec y MyAlert** y el apoyo estratégico de la Asociación de Internautas, se presenta el primer servicio de alertas de virus y seguridad informática vía SMS que todos los usuarios podían recibir gratis. Un sistema de alertas adelantado a su tiempo que desaparecería sólo un año después.

_ La **Agencia de Seguridad Nacional (NSA)** norteamericana hace pública una versión "segura" del popular sistema operativo Linux. Varios organismos oficiales norteamericanos habían demostrado interés en disponer de un sistema operativo de calidad y seguro, con código fuente, para poder hacer frente a la eventualidad de que desapareciesen los sistemas actualmente en uso, como Trusted Solaris (Sun), Trusted AIX (IBM) o Trusted IRIX (SGI, antigua Silicon Graphics). La NSA norteamericana hace pública una versión de Linux que cumple los criterios "Trusted", basada en el kernel Linux 2.2.12 y en la distribución RedHat 6.1, bajo licencia GNU GPL (GNU General Public License).

Una al día



02/01/2000 Efecto 2000: éxito sin precedentes y verdades a medias

Pese a que esperamos surjan nuevos incidentes a causa del efecto 2000, la escasa incidencia de problemas en los servicios críticos a nivel mundial hace pensar en el éxito de las medidas adoptadas. En estos momentos, mientras algunos hasta se plantean la gravedad real del problema, es cuando no podemos -ni queremos- pasar por alto el enorme esfuerzo de miles de personas en la lucha contra el mayor desastre potencial de la historia informática: felicidades. Aun queda por ver el impacto final que supondrá el efecto 2000 en los sistemas, existen procesos administrativos donde los incidentes pueden tardar semanas o meses en salir a la luz. Pero una vez pasadas las primeras horas, donde se temía por los sistemas más críticos, el efecto 2000 nos ha dejado algunas enseñanzas: el mundo está más conectado de lo que muchos preveían, la tecnología actual permite afrontar retos globales de forma eficaz, y la principal "culpable" es Internet.

Incidentes que no salen a la luz pública

Aunque los incidentes reportados hasta el momento no son excesivamente numerosos ni graves, no significa que en realidad no se estén dando mas casos de sistemas afectados. La información de la que disponen los medios es facilitada, en la mayoría de los casos, por los gabinetes de crisis de los gobiernos, desde donde se está ejerciendo un estricto filtro sobre las notificaciones. A este contratiempo mediático, hay que sumar que muchas compañías privadas tienen contratos de confidencialidad, por lo que tampoco pueden suministrar datos sobre las actuaciones que se están llevando a cabo en estos momentos.

Por poner algún ejemplo, Gartner Group afirma haber recibido durante media jornada cerca de 400 incidentes Y2K desde pequeñas y medianas empresas. Por supuesto, ellos no pueden ofrecer más datos, ya que tienen firmados contratos de confidencialidad con sus clientes.

En España, aunque todos debemos felicitarnos por los resultados hasta el momento, el panorama no es muy diferente. Se están trabajando en incidentes en distintas empresas y organismos, si bien estos

problemas no saltan a la luz pública por la rápida actuación de los técnicos y por no afectar a los servicios externos. Por los comunicados oficiales del gobierno todo parece indicar que no se ha dado ningún caso, contrastando, por ejemplo, con una de las últimas filtraciones a los medios de comunicación fuera de nuestro país, donde se habla de problemas derivados del efecto 2000 en centrales nucleares de España.

Dudas sobre el Efecto 2000

Nos ha sorprendido, tristemente, que desde algunos foros, supuestamente de carácter informático, se haya insinuado la inexistencia del problema o intentado minimizar. Desde un punto de vista técnico el problema es palpable, así como su implicación en la mayoría de los procesos críticos y administrativos. Si bien no hay que dar mayor importancia a esos comentarios ya que, como viene siendo habitual, no aportan ningún dato técnico o base teórica, y simplemente se excusan en suposiciones subjetivas en base a que no hay incidentes graves. Parece ser que para algunos es imposible que los informáticos hagan bien su trabajo, o simplemente esperaban que el efecto 2000 terminara por estropearles la tostadora.

Sobredimensionamiento y "defectos secundarios"

Otros comentarios y artículos, aunque con un enfoque distinto a nuestro planteamiento, si han merecido la reflexión de la comunidad y nuestra participación activa en algunos foros de discusión. En estos casos la atención se ha centrado sobre los medios que han generado psicosis en la población con alarmas innecesarias, sobredimensionando el alcance de los posibles incidentes, así como en el gasto que ha supuesto las medidas adoptadas desde los gobiernos y el enriquecimiento de empresas que han aprovechado la confusión. Si bien aceptamos en parte, y con matices, dichos planteamientos -sigue siendo complicado y oportunista hacer valoraciones a posteriori sobre temas tan subjetivos- hemos querido dejar constancia de que estos "defectos secundarios" no deben empañar el esfuerzo y dedicación de los profesionales, ni la gravedad del problema original.

Bernardo Quintero

21/01/2000 El gobierno reformará la ley para evitar el delito informático

Según expuso el Ministro de Interior Jaime Mayor Oreja el gobierno tiene intención de adaptar la ley para luchar contra la proliferación del delito informático. El Ministro de Economía Rodrigo Rato también confirmó este dato en las jornadas sobre seguridad en la economía digital organizadas por la Guardia Civil. Según el ministro de Interior la evolución que manifiesta Internet así como el mayor de volumen de transacciones electrónicas a través de la Red obligará al Gobierno del PP, caso de ganar las próximas Elecciones Generales, a legislar con agilidad y a su vez esas leyes deberán estar sujetas a continuos cambios. Todo ello debido a la evolución continua de la Red y el modo de cometer delitos dentro de ella.

Entre los asistentes a estas jornadas se ha hecho especial hincapié a la protección de la propiedad intelectual y garantizar la seguridad en las transacciones electrónicas. Algunos de los datos fueron aportados por destacados nombres dentro de la sociedad informática española, como Francisco Román, director general de Microsoft, que afirmó que España es uno de los países europeos con mayor índice de piratería.

El Coronel de la Guardia Civil Manuel Nieto dio a conocer el dato que de los 125 casos investigados por la G.C. en estos tres últimos años se han resuelto el 90%. También destaco que el delito que está tomando mayor auge es el de la utilización fraudulenta de tarjetas de crédito a través de Internet. Para esto se

utilizan diversos medios, como la obtención de recibos tirados por los usuarios en papeleras, la difusión de listas de números a través de la Red, generadores de números válidos, etc.

Antonio Román

23/02/2000 Virus “in the wild”, ¿cuál es la fórmula?

En muchas ocasiones diversos especialistas han tratado de extraer conclusiones a partir de las llamadas “wildlists”, con el fin de poder intuír de antemano cuáles serán los virus o i-worms de mayor prevalencia a corto plazo. Las estadísticas que revela este tipo de listas, sin embargo, aún dejan muchas incógnitas pendientes. Para muestra, un botón: la producción de virus de fichero para Win32 es, desde hace meses, sensiblemente superior a la de virus de macro, i-worms y, por supuesto, especímenes infectores del ya vetusto DOS. Sin embargo, y de acuerdo con los datos ofrecidos a partir de la última “wildlist” oficial, el único representante de este grupo de cuya actividad infecciosa se tiene constancia es el “CIH”, que, eso sí, con 38 impactos, se sitúa segundo en la lista, detrás del aparentemente imbatible “Happy99”.

Esta situación viene a ser una continuación de la relación que ya protagonizaron los virus de fichero de DOS y los prácticamente desaparecidos infectores de “boot”: a pesar de que los primeros eran cuantitativamente superiores, los segundos siempre llevaron la delantera en cuanto al número de infecciones producidas a nivel mundial.

Lo cierto es que resultaría increíblemente tedioso efectuar una valoración para dilucidar si el problema atiende a razones de mayor o menor complejidad, si bien es cierto que, en líneas generales, los virus de fichero suelen ofrecer aspectos de tipo técnico más interesantes que los que podemos encontrar en los especímenes infectores de “boot”. Pero este argumento chocaría de golpe con un hecho tan peculiar como el que representa la presencia del virus “Form”, simple y directo donde los haya, año tras año y mes tras mes en puestos privilegiados de las listas de prevalencia, compartiendo cartel con un clásico de fichero como “OneHalf” -conocido por ser uno de los virus de DOS más complejos que se recuerdan y con “AntiCMOS” y “AntiEXE”, dos ejemplares más de “boot” cuyo estilo raya en el más puro de los minimalismos. El testigo de “OneHalf” parece recogerlo el “CIH”, que en su momento fue un auténtico impacto técnico - poca gente hasta entonces había sido capaz de alcanzar “ring-0” (el anillo de privilegios máximos en Windows) desde un virus.

Entonces... ¿tienen más posibilidades de extenderse “in the wild” los virus de “boot” simples y los virus de fichero más complejos? ejemplos como “Marburg” -un infector de archivos de formato PE EXE para Windows95 bastante simple- o “Zhengxi”, considerado como uno de los virus de fichero más complejos de la historia, no son más que la punta del iceberg que desbarata cualquier tipo de teoría al respecto.

Por si esto fuera poco, los virus de macro, relevo generacional de los infectores de “boot”, crecen en progresión geométrica mes tras mes, y siguen siendo, con mucho, el género de virus más extendido desde su aparición. Estadísticas oficiales hacen eco de un dato alarmante: más del 65% de las infecciones que tienen lugar a diario están producidas por un virus de macro, y de hecho es posible comprobar cómo, de los diez especímenes más extendidos de acuerdo con la “wildlist” del mes de enero, seis pertenecen a este simple pero muy efectivo género vírico.

Sin embargo, el verdadero problema lo tenemos a la vuelta de la esquina: el fenómeno de los gusanos (i-worms e IRC worms) está cobrando un peligroso protagonismo, pese a su corto periodo de vida.

Especialmente en el caso de los i-worms, habría que hacer hincapié en un hecho escalofriante: el primer espécimen de este tipo data de enero de 1999, y, desde entonces, se han escrito menos de quince ejemplares de este género. Sin embargo, cuatro de ellos aparecen en los primeros puestos de la “wildlist” del mes de enero (entre ellos, “Happy99” en el primer puesto), y se tiene constancia que la práctica totalidad de los restantes i-worms conocidos hasta el momento han sido encontrados en algún momento “in the wild”.

Las estadísticas que se barajan, en comparación con las de los géneros de virus más antiguos, nos hacen augurar un futuro muy poco esperanzador. El clavo ardiente al que debemos agarrarnos es el hecho de que, salvo el caso de “BubbleBoy”, la ejecución de un i-worm en un ordenador no infectado es una situación de interacción en la que se miden las fuerzas los recursos a nivel de ingeniería social de los escritores de virus y la precaución de los usuarios, que, en el momento de recibir un gusano pasan automáticamente a convertirse en posibles víctimas.

A pesar de todas estas conjeturas, siempre nos quedará una duda por resolver: ¿hasta qué punto dependen las probabilidades que tiene un virus de cara a su ulterior expansión “in the wild” de sus mecanismos de auto-ocultación? ¿cuándo y cómo se suele descubrir la mayoría de las infecciones víricas? ¿tras haber escaneado el disco duro con un antivirus actualizado, o antes de que el propio antivirus haya tenido noticia de la existencia del espécimen en cuestión? y, sobre todo, ¿cuántas infecciones víricas se han producido a lo largo del mundo y siguen vigentes hoy día sin haber sido descubiertas?

Las estadísticas son un dato fundamental de cara a la futura prevención de males que hoy en día nos aquejan, y por desgracia son todavía muy pocas las compañías antivirus que se preocupan por obtener algún tipo de información adicional por parte de sus usuarios acerca de los ataques víricos que éstos sufren día tras día, algo que puede suscitar dos últimas preguntas: ¿hasta qué punto interesa a este tipo de empresas erradicar de manera definitiva las plagas víricas de la informática? ¿funcionan de manera análoga a la medicina general, prestando más atención a las consecuencias que a las causas reales?

Giorgio Talvanti

06/04/2000 Las guerras de los MP3

¿Acabará el formato MP3 y la distribución de música a través de Internet con la industria discográfica? Para muchos la respuesta es un contundente y rotundo SÍ. La única duda resta en saber exactamente en cuánto tiempo.

Esta industria multimillonaria se ha caracterizado por aplastar todas las tecnologías que potencialmente podían amenazar sus vastos intereses económicos. Primero destruyó el formato DAT y cuando MP3 se extendía peligrosamente, su reacción no se hizo esperar: en cuanto Diamond (www.diamond.com) lanzó al mercado su controvertido reproductor Rio, la RIAA (Asociación Americana de la Industria Discográfica), que representa a los principales sellos discográficos del mundo, llevó a la compañía a los tribunales alegando que la venta de Rio alentaría la piratería. El veredicto final, emitido en junio de 1999, declaró que Rio no violaba ninguna ley ni la AHRA (Audio Home Recording Act), en la medida en que el reproductor copia las canciones directamente de un ordenador y no desde un CD original. Este veredicto se consideró una gran victoria de MP3 sobre la voraz industria discográfica. A continuación, RIAA se volvió contra MP3.com (www.mp3.com), el mayor sitio web de distribución de música comprimida. En enero de 2000, la asociación de discográficas demandó a MP3.com por supuesta infracción de derechos de autor de más de 45.000 CD de música, ofrecidos a través de su servicio My.MP3 en circunstancias que

poco tenían que ver con las acusaciones. Por su parte, MP3.com demandó a RIAA un mes después por prácticas comerciales desleales, difamación, libelo, e interferencias con posibles ganancias económicas. Otros demandados por RIAA han sido Lycos (caso perdido también) y Napster (probablemente, perdido también). Los defensores de MP3 y la música en Internet se preguntan, ¿a cuántos más debe demandar la RIAA antes de darse cuenta de que su guerra está perdida?

¿Qué guerra? Cuando el canal de distribución primario era el CD, las cosas estaban atadas y bien atadas. ¿Que alguien graba un CD a cinta? No supone una amenaza, al fin y al cabo, la calidad es menor. Poco después hacen su aparición los copiadores de CD-ROM. ¿Que la industria discográfica afronta pérdidas por piratería? Tampoco pasa nada, al fin y al cabo, todos están metidos en el mismo cotarro y son los que venden los aparatos, los CD vírgenes y demás: se grava a los CD vírgenes con un canon para afrontar las pérdidas y los ingresos vuelven a su cauce. ¿Que el artista sale perdiendo? Qué se le va a hacer.

Sin embargo, la distribución de música a través de Internet, que gracias al formato de compresión de MP3 permite su rápida descarga y almacenamiento en disco, hace tambalear los cimientos de este emporio. La primera solución buscada consistió en luchar contra MP3, pero no se puede escupir a las cataratas del Niágara. Al fin y al cabo, a lo mejor hasta se puede sacar tajada de Internet. Vivimos en plena fiebre de pelotazos, ¿no?

"Si no puedes con ellos, únete a ellos", dice el refrán. La RIAA, con su Iniciativa para la Música Digital Segura (SDMI), está intentando poner freno a la distribución incontrolada del MP3, pero sin renunciar a sus nuevas oportunidades de negocio a través de Internet. La SDMI, lanzada por RIAA y que reúne a más de 160 compañías y organizaciones, entre ellas sellos discográficos (como los gigantes EMI o Warner), compañías de electrónica y de TI, proveedores de servicio de Internet y compañías de tecnología de seguridad, ha estado trabajando en la creación de un estándar para la protección de música en MP3 y otros formatos. Hasta el momento, en su Fase I, la SDMI ha acordado adoptar la tecnología de Verance Corporation (www.verance.com), llamada Musicode, para la inserción de marcas de agua robustas en las obras musicales. La Sociedad General de Autores y Editores (SGAE) ha firmado en diciembre del año pasado un acuerdo con Verance, que licencia a la SGAE para que utilice la tecnología MusiCode de Verance para incluir marcas de agua inaudibles en las obras musicales de sus miembros y monitorizar automáticamente sus difusiones públicas por radio, TV e Internet. De esta forma, la alianza entre SGAE y Verance supone un hito en la historia de la moderna lucha contra la piratería digital.

En el futuro, los reproductores MP3, incluido Rio, que cumplan con las especificaciones de la SDMI, sólo serán capaces de reproducir la música grabada legalmente, dotando así a las compañías discográficas de mayor control sobre sus materiales protegidos. Con esta iniciativa, la RIAA pretende adoptar un marco común para que artistas y empresas de tecnología y sellos discográficos puedan utilizar Internet como nuevo canal de distribución, novedoso y potencialmente muy beneficioso. Eso sí, velando por la protección de los derechos de autor legítimos.

Queda por ver la aceptación que tendrán estas nuevas medidas entre el público y las pequeñas casas y distribuidoras y tiendas de música. ¿Se pretende salvaguardar las ventas de los grandes sellos, que ven amenazada su posición de abuso con la democratización de las tecnologías de copia y reproducción de música, o proteger los derechos de autor de los artistas? La criptografía no da respuestas a estas preguntas, ofrece herramientas para proteger la propiedad intelectual, como las marcas de agua, pero nunca infalibles. Y si no, que le pregunten a Stephen King.

Gonzalo Álvarez Marañón

04/05/2000 Consideraciones sobre VBS.LoveLetter, un gusano muy simple

Pese a la fiebre mediática que ha desatado, merecida sólo en parte por la propagación que ha conseguido, a la postre la mayor de toda la historia, debemos de tener en cuenta que en realidad se trata de un script que ha de interpretarse, un gusano muy simple, con su código al descubierto, que analizaremos al detalle en una próxima entrega.

No hay un antes y un después de este gusano, al menos en el apartado técnico, aunque la eficacia conseguida a la hora de propagarse, gracias en gran parte al factor humano, tal vez sea utilizada como excusa para implantar nuevas medidas y restricciones en las políticas de seguridad y control.

En cuanto a las casas antivirus, por un lado sólo cabe felicitarlas por su rápida actuación, apenas unas horas después los clientes contaban con actualizaciones para detectar y eliminar el gusano, y hasta se han facilitado utilidades gratuitas para los usuarios no registrados.

Por otro lado, mientras las casas de software hacen su particular agosto, más de uno se preguntará como es posible que un gusano tan simple, con técnicas conocidas, ha podido atacar por igual a los que disponían de un antivirus actualizado como a los que iban a "pecho descubierto". El modelo actual de los antivirus es eficaz contra virus conocidos, promesas de anuncios y heurísticas al margen, hoy día sigue siendo muy fácil saltarse esta barrera de protección que casos como el de VBS.LoveLetter ponen en entredicho.

Internet se ha convertido en todo un handicap para los antivirus, si bien es cierto que han ganado en capacidad de actualización, los virus tampoco dejan de aprovechar las ventajas de la Red, pudiendo propagarse por miles de sistemas antes que los laboratorios hayan terminado de analizar el espécimen.

El modelo de detección de virus conocidos, resolutivo en épocas pasadas cuando la infección entre sistemas aislados se producía, por ejemplo, al intercambiar disquetes, pierde eficacia cuando el ciclo de propagación entre millones de máquinas vía Internet se reduce a unas pocas horas. La realidad es que existen soluciones de seguridad más efectivas, basta que las empresas de software se planteen las necesidad de una pequeña revolución.

Dejando al margen los antivirus, necesarios y recomendables, así como a Internet, de cuyo beneficio nadie duda, VBS.LoveLetter pone de nuevo el dedo en la llaga: la inseguridad de Microsoft. Una vez más los usuarios de Linux se han convertido en meros espectadores, protegidos por un modelo de seguridad mucho más robusto que el de Windows, y donde los virus, hasta la fecha, son simples anécdotas.

En el último escalón nos encontramos con el factor humano, que es sin duda el gran protagonista en el caso de VBS.LoveLetter, donde la Ingeniería Social de este simple gusano ha obtenido mejores resultados a la hora de propagarse que las complicadas técnicas desarrolladas bajo ensamblador de otros virus mucho más sofisticados. Una vez más, es en última instancia el usuario quién tiene en su mano la seguridad de los sistemas, y quién debe ser consciente y responsable del peligro que entrañan sus acciones en determinadas situaciones.

Bernardo Quintero

12/07/2000 Carnívoro

Carnívoro es el nombre del nuevo invento del FBI. Resulta un poco “gore”, asusta sólo el nombrecito y, lo que puede hacer también. Vigila, intercepta y analiza grandes cantidades de correo electrónico, va más allá de lo que imaginó la propia ley sobre Privacidad en Comunicaciones Electrónicas (ECPA).

Esta semana he recibido varias cartas interesantes, una de ellas me habla de Carnívoro y me adjuntan la misiva enviada por Laura W. Murphy, Barry Steinhardt, y Gregory T. Nojeim, cúpula directiva de ACLU, (American Civil Liberties Union), a varios representantes del pueblo norteamericano, los honorables Charles T. Canady, y Melvin L. Watt. Carta que deja clara la protesta por la existencia misma de dicho Carnívoro que segun los autores de la carta podría incluso violar la Cuarta Enmienda.

Al parecer de la existencia de Carnívoro ya se sabía desde el 6 de abril, básicamente un software muy especializado instalado directamente en los propios ISPs, (Internet Service Provider’s), o proveedores de servicios, que intercepta en tiempo real los contenidos de las comunicaciones individuales,permite el acceso a todo el correo de todos los clientes del ISP, y de todas personas que comuniquen con dicho proveedor, las copia, tracea y registra, basta con darle una o varias palabras a buscar en cada correo.

Carnívoro accede a todo el trafico del ISP, y no sólo a las comunicaciones. Según los autores de la carta, Carnívoro analiza millones de mensajes por segundo, reteniendo sólo los que tengan determinadas palabras buscadas, hace su trabajo sin informar, después al ISP (antes sí, ya que puede ser obligado a instalar el programa). Y lo peor de todo, sin informar antes al Juzgado. Aunque no lo sepan algunos, también en Estados Unidos es necesaria una orden judicial para tal tipo de comportamiento.

El FBI asegura que sólo graban lo que tiene un perfil determinado, y sobre la necesidad de orden judicial para ello, vienen a contestar, algo así como “creed en nosotros, somos lo buenos, los chicos del gobierno”. Como principio general en las legislaciones occidentales la interceptación de comunicaciones debe ser algo excepcional, no habitual, debe minimizarse, para un tiempo, persona y conducta determinada, y por supuesto debe estar autorizada por el Juez, Carnívoro obviamente hace todo lo contrario.

En España se pueden ver como derecho material los art. 197 y 536 del Código Penal, o en jurisprudencia las sentencias del Tribunal Constitucional 107/85, la 64/86, la 49/96 de 26 de marzo, la 34/96 del 11 de marzo; el auto del Tribunal Supremo 18/6/92, o la sentencia del mismo órgano de 23/11/95, la de 28/3/96. Y ello sólo para empezar.

Para los miembros de ACLU sería ilegal, (legislación norteamericana), que el gobierno pueda obtener de un ISP las entradas y salidas de correo de un cliente, dirección de correo, IP, etc., consideran también ilegal que los ISPs puedan ser obligados a instalar semejante “trampa” en sus máquinas. Para el ACLU la cuarta enmienda prohibiría tal cosa, ya que prohibe el acceso a los contenidos, incluida la “subject” del mensaje, el cual es ya contenido.

El FBI ya no necesita ni a Kevin Mitnick, que aunque salió de prisión en enero, sólo desde el día 10 de Julio la Juez Federal Marianne Pfaelzer le permite contestar a algunas de las ofertas de trabajo recibidas, alguna de ellas en el campo de la seguridad informática; e incluso, ya puede escribir sobre materia tecnológica y hablar en público, ya lo ha hecho en la KFI, radio de Los Angeles.

Lástima no le preguntaran su opinión sobre Carnívoro. Total, por cosas similares él fue a la cárcel, en cambio otros, ni siquiera dimiten.

Eusebio del Valle

18/09/2000 Aparece el primer virus “companion” para NTFS

Hace apenas unas semanas el mundo de los virus informáticos volvía a experimentar una revolución en el campo de la investigación y el desarrollo de nuevas técnicas de infección; en esta ocasión se ha tratado de “Stream”, que pasará a la historia por ser el primer patógeno de tipo “companion” nativo para sistemas de tipo NTFS.

La inmensa mayoría de los virus informáticos, desde la aparición de “Brain” en 1986, se puede subdividir en dos grandes grupos, en función del tipo de infección aplicada a los ficheros “huésped” o víctimas del contagio: “appending” (anexión del código maligno al final del archivo), la más común, especialmente con la llegada de los sistemas de 32 bits, y “prepending” (adhesión del cuerpo del virus antes del código original), característica de un nutrido grupo de especímenes experimentales de las primeras oleadas en la era del DOS.

Otros métodos menos convencionales pero también frecuentados por diversos autores han sido el de “overwriting” (sobreescritura del fichero huésped con el código vírico) y el de “spawning” o “companion”, consistente en sustituir un programa original con una copia del virus que, al ser ejecutada, se encargará de correr la aplicación huésped, previamente renombrada y escondida de los ojos del usuario afectado.

El origen de esta técnica de infección -que generalmente conserva intacto e íntegro el código de los ficheros originales- se puede encontrar en la jerarquía ejecutiva prevalente en el DOS, mediante la cual un fichero de extensión COM con idéntico nombre que uno de extensión EXE estaba dotado de preferencia. Así, se daba la circunstancia de que si el usuario ejecutaba “programa” -sin especificar extensión alguna- y existían los ficheros de nombre “programa.exe” y “programa.com”, era este último el primero en el orden de ejecución.

Aprovechándose de esta característica, los virus “companion” más antiguos lo tenían tan fácil como buscar archivos de un tipo determinado de extensión y renombrarlos, creando una copia de su propio código con el nombre original del fichero afectado, de forma que la carga maligna sea ejecutada cada vez que el usuario desee correr un programa, que acaba siempre por ser lanzado por el propio virus, tras haber llevado a cabo sus menesteres.

Años más tarde, cuando una técnica de semejante primitivismo ya había quedado desfasada, los autores de virus han vuelto a darle la vuelta a la tortilla y han encontrado una manera de volver a dar vida a un resorte de tecnología vírica que había caído en el olvido; uno de los programadores de “Stream”, el checo “Benny”, ya había pasado a la posteridad meses antes tras su participación en la escritura de “Install”, el primer virus para Windows2000.

La adaptación del mecanismo “companion” puesta en práctica por el virus “Stream” ha sido ya bautizada como “stream companion”, de donde el patógeno ha tomado su nombre. Se trata de un método de infección válido única y afortunadamente para ordenadores con sistema de ficheros NTFS, el que emplean, principalmente, tanto WindowsNT como Windows2000. El motivo radica en el hecho de que en estas plataformas ha sido habilitado por Microsoft, su desarrollador, un complejo mediante el cual cada fichero posee un flujo de datos o “data stream” al que se pueden asociar otros elementos análogos, accesibles mediante su nombre personal, que responde al formato “nombre_fichero:nombre_flujo”.

La asociación de un flujo con su fichero es permanente, y así, resulta imposible de acceder o modificar sin previa referencia a su “compañero”, al que permanece “grapado” incluso si éste es renombrado o borrado, algo que complica sobremanera la detección de “Stream”, al no existir herramientas incluidas por defecto

en el sistema para editar o visualizar los flujos de un archivo.

Lejos de tratarse de una técnica de implementación laboriosa, la longitud del código de este patógeno es tan insignificante como irrelevante, especialmente tras haber sido procesada por el compresor "Petite", que reduce el tamaño de "Stream" a tan solo cuatro kilobytes. Al tratarse de un espécimen de carácter experimental, de su acción expansiva potencial podría decirse que se encuentra en relación directamente proporcional con la longitud del virus: su acción maligna se limita a intentar infectar todos los ficheros del directorio actual. En caso de fallo, "Stream" muestra el siguiente mensaje en pantalla:

[Win2k.Stream by Benny/29A & Ratter]
This cell has been infected by [Win2k.Stream] virus!
[OK]

La rutina de contagio, por su parte, se limita a acceder a cada uno de los ficheros encontrados y a copiar el código original en un nuevo flujo, de nombre "STR", sustituyéndolo en el "stream" principal por una copia del virus, que, tras ser ejecutada, se encarga de ceder el control al archivo huésped, accesible por medio de la ruta "nombre_fichero:STR". Como nota anecdótica cabría resaltar que -por motivos hasta ahora desconocidos- a pesar de que la técnica de "stream companion" es perfectamente compatible con WindowsNT, los autores de "Stream" incluyeron en el código de su creación una rutina que le impide correr en otras versiones del sistema operativo de Microsoft distintas a Windows2000, reduciendo aún más si cabe el posible radio de acción del virus en caso de ser liberado.

Giorgio Talvanti

27/10/2000 Caso Microsoft: debilidades en el planteamiento

La filtración original en el Wall Street Journal, de una fuente no identificada, sitúa al troyano "Qaz" como la herramienta usada por los atacantes para introducirse en la red interna de Microsoft. Este rumor no confirmado se ha convertido en la hipótesis "oficial" a la que medios y "expertos" han recurrido para explicar el ataque. Vamos a ver sus principales puntos débiles, tanto de la hipótesis como del troyano, que lo convierten en una herramienta que ni siquiera cumpliría su objetivo contra la red de cualquier mediana empresa.

- ¿Cómo funciona "Qaz"?

"Qaz" es un ejecutable Win32, escrito en Visual C++. Cuando se ejecuta, busca una copia del fichero NOTEPAD.EXE (Bloc de Notas de la carpeta Windows) y lo renombra como NOTE.COM, a continuación "Qaz" se copia con el nombre de NOTEPAD.EXE. Esto provoca que, cada vez que se intente lanzar el Bloc de Notas en un sistema infectado, primero se ejecuta el troyano, y éste a su vez llama a NOTE.COM, por lo que el usuario no percibe a primera vista ninguna irregularidad. El troyano es capaz de propagarse a través de las unidades compartidas de las redes locales, donde intenta localizar la carpeta de Windows, para lo cual, busca la cadena "WIN", y realiza con NOTEPAD.EXE la misma operación ya descrita. Por último, destaca en "Qaz" su funcionalidad como backdoor, envía la dirección IP de los ordenadores infectados a su autor vía correo electrónico (a buzones localizados en China originalmente), y abre una puerta trasera en el puerto TCP 7597, por el cual el autor del virus puede acceder de forma remota al sistema de sus víctimas.

- La víctima: el empleado de Microsoft

En una red local los ordenadores no se conectan directamente a Internet, sino que cuentan con un servidor proxy a través del cual se comunican con el exterior, ya sea para recoger/enviar correo, visitar páginas webs o cualquier otra conexión. Este esquema también supone un primer nivel de seguridad, al impedir las conexiones directas desde/hacia el exterior, y es el mismo que cualquier pequeña o mediana empresa utiliza para aprovechar la conexión de varios ordenadores mediante una única línea telefónica.

- Problema en el planteamiento

En el caso de que “Qaz” infectara un ordenador de una red local, ejemplo Microsoft, el troyano abriría en esa máquina el puerto TCP 7579 y enviaría a continuación la dirección IP local de la víctima al atacante por correo electrónico a través del proxy. Una vez recibida la dirección IP, el atacante no puede conectarse a ese ordenador, ya que esa IP es interna y no está accesible desde Internet. Cuando se trata de un usuario particular, que accede de forma directa a Internet, “Qaz” si se muestra efectivo.

- ¿Podría el atacante conocer la dirección del servidor proxy?

De forma fácil, ya que podría recibir la dirección en la cabecera del mensaje de correo electrónico que manda “Qaz”. El atacante si podría intentar interactuar con la dirección IP del proxy, si bien no podría acceder remotamente por la puerta trasera vía TCP 7579, ya que el proxy no se encuentra infectado.

- Si “Qaz” se transmite a través de las redes locales, ¿no podría haber infectado al servidor proxy?

“Qaz” sólo se transmite entre las unidades compartidas de una red local. Un proxy por defecto, bien configurado, no debe compartir su unidad sin ningún tipo de protección.

- Bueno, tal vez el proxy de Microsoft estuviera mal configurado, ¿no?

En cualquier caso, sería necesario que compartiera toda la unidad con acceso lectura/escritura (un error aun menos probable), ya que “Qaz” busca la carpeta de “Windows” para escribir en ella la copia del troyano.

- Vale, aunque imposible, supón que hubiera llegado allí

“Qaz” no es capaz de ejecutarse a través de la red local, sólo sitúa el fichero infectado en una posición óptima para que un usuario lo ejecute (simulando al bloc de notas). En el caso del servidor proxy de una gran empresa no hablamos de un terminal que se utilice como una estación de trabajo por un usuario, sino de un servidor dedicado, lo que dificultaría también que se ejecutara.

- Bueno, una posibilidad entre 1 millón, pero pudo darse, ¿no?

Hasta ahora sólo habíamos hablado del servidor proxy cómo escalón de seguridad, en cualquier empresa con una política de seguridad mínima debemos de contar con la figura del cortafuegos que filtra las conexiones en base a una configuración, cómo mínimo se limita el acceso sólo a través de unos determinados puertos. Un troyano tan limitado como “Qaz” tampoco salvaría este obstáculo, el cortafuegos impediría la conexión desde el exterior.

- ¿Existen más puntos en contra?

Si, “Qaz” es un troyano conocido desde principios de agosto, la mayoría de las casas antivirus detectan

y eliminan desde entonces este espécimen. Muchas empresas utilizan distintos niveles de protección antivirus, que llegan hasta el chequeo de los mensajes de correo electrónico en el servidor, lo que hubiera impedido que llegara el troyano al empleado de Microsoft.

- Bueno, tal vez se utilizó contra éste empleado en un primer momento, antes que las casas lo identificaran y detectaran. La versión original de "Qaz" enviaba los mensajes de correo electrónico a una cuenta de China, en este caso se trataría de una versión modificada (posterior) que un atacante configura para beneficio propio. Aunque se hubiera utilizado antes de que los antivirus lo incluyeran en su base de datos de firmas, un antivirus local con una actualización más o menos reciente lo habría detectado a posteriori.

- ¿Es normal que un "hacker" (deberíamos decir "cracker") de cierto nivel, cómo para comprometer a Microsoft, utilice un troyano de estas características?

No, cualquier atacante de cierto nivel programará las herramientas de forma personalizada, lo que le permite ajustarse a las necesidades de la operación y asegurarse de que ningún antivirus va a detectarlo cómo "malware".

- ¿Es posible que con un esquema similar, evitando las debilidades intrínsecas de "Qaz", se haya podido llevar una intrusión en la red de Microsoft?

Si, hay muchas formas de vulnerar la seguridad de una red, sobre todo en entornos basados en los productos de Microsoft. Es posible realizar un ataque similar, más efectivo, basado en las propias debilidades de Windows, sin necesidad de una cabeza de turco como "Qaz".

- ¿Por ejemplo?
En la próxima entrega.

Bernardo Quintero

Entrevista


Juan Salom

Juan Salom es el Jefe del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil desde el 2000. Hispasec siempre ha colaborado con ellos en lo que han estimado oportuno. Resulta muy sencillo ayudar a personas que están siempre dispuestas a aprender y aprecian tanto su trabajo. Su labor cuenta con muchos éxitos en la lucha contra el fraude online y la difusión de pornografía infantil.

Hispasec: ¿Cuándo y cómo se creó el Grupo de Delitos Telemáticos?

Juan Salom: El Grupo de Delitos Telemáticos fue creado a finales del año 1.996, encuadrado dentro de la Unidad Central Operativa de la Guardia Civil. Tras una serie de investigaciones que pusieron en evidencia la necesidad de especializar personas en la investigación informática, a finales de ese año, se constituyó el embrión del actual Grupo de Delitos Telemáticos de la Guardia Civil. Compuesto por cuatro agentes y un oficial que combinaban experiencia investigadora y conocimientos informáticos, empezó a andar la unidad. Trabajo no le faltó, y enseguida llegaron los primeros éxitos. Operaciones como TOCO e HISPAHACK, tuvieron un importante eco mediático, no tanto por su dificultad como por su novedad. El concepto de "ciberpolicía" empezaba a asentarse. La pequeña unidad de Delitos Informáticos pedía pan y había que darle de comer. Su plantilla se duplicó y llegaron más servicios.

H: ¿Cómo te metiste en esto?

JS: El esfuerzo inicial estaba hecho y la factura de ese trabajo personal fue muy alta. Quizá por eso, su jefe, un entrañable amigo, decidió pasar el testigo. Rondaba el inicio del año 2000. Casualidades de la vida me llevaron a optar a ese puesto. Yo era un hombre de investigación. Me había curtido como oficial e investigador en otras lides. Acababa, como quien dice, de llegar a Madrid. Mi misión era otra, el blanqueo de capitales. Recién empezaba en ese mundo y de repente la suerte llamó a mi puerta. Y digo suerte con la perspectiva de los años, entonces era el reto. ¿Qué sabía yo de informática? Un aficionado, de esos que se identifican en las entrevistas con el triste "conocimientos a nivel usuario". Pero los retos me atraen y la ignorancia es muy atrevida. Y allí me lancé, a intentar hacerlo lo mejor que supiera.

Lo primero que hice, lo que hace todo jefe para que se note que ha llegado, fue mover la mesa y cambiar el nombre de la unidad. Nos llamaríamos Grupo de Delitos Telemáticos. Hoy se mantiene el nombre, lo que significa que continúo en el puesto. Después, seguir los consejos de mi antecesor, que fueron pocos pero precisos: Léete este libro que te permitirá conocer los conceptos básicos de redes, procura estar al día en las innovaciones que van apareciendo y déjate ayudar por todos aquellos que nos quieren y nos valoran.

Y así empecé las interminables horas de estudio con el modelo de protocolos OSI, con los TCP/IP, las tipologías de redes,... hasta que entendí mínimamente, o eso creía yo, qué era eso de la red de redes, Internet, y los distintos servicios. Los siguientes pasos fueron buscar las fuentes para mantenerme actualizado en mis escasos conocimientos y a ser posible incrementarlos, y conocer a todos aquellos que pudieran y quisieran apoyar a los "ciberpolicías" de la Guardia Civil. Y ahí entrasteis vosotros, Hispasec con Una-al-día. Desde entonces me habéis acompañado en mi viaje de dirección de un grupo de investigación informática.

H: ¿Cuál fue tu primer contacto con Hispasec?

JS: Por aquel entonces, desde mi ignorancia (que aún mantengo) alucinaba con Una-al-día. ¿Cómo es posible que alguien escriba todos los días sobre un tema tan técnico? ¿Habrá tantas noticias? Hoy sigo alucinando, no por el hecho de escribir todos los días, que con la cultura de la web 2.0, es algo ya superado, sino con la calidad técnica y claridad de los artículos. La lectura diaria de vuestras noticias no hacía más que incrementar mi admiración por vosotros. Y para colmo, otros foros del mundo de la seguridad TIC, repetían vuestras noticias.

Por el papel que me ha tocado jugar, mi ámbito de relaciones en este mundillo se iba ampliando y mi presencia era reclamada en distintos foros que deseaban conocer la respuesta que daba la Guardia Civil frente al problema de la delincuencia informática. Y allí donde acudía, cuanto más técnico era el encuentro, allí encontraba referencias a Hispasec. Hasta en Sudamérica se os conocía. Hubo un momento, de verdad, que me planteé como objetivo táctico el contactar con vosotros. Y si antes lo pienso, antes surge la ocasión. Un buen día, allí por el año 2003, se recibe en la cuenta de correo del Grupo de Delitos Telemáticos un mensaje informando sobre un presunto ataque a los servidores de Hispasec. En cuanto me pasaron el mail, le di la máxima prioridad. Esa era mi brecha y debía aprovecharla. Y para Málaga que me fui. Eso sí, acompañado de mi hombre más técnico y temeroso de encontrarme y enfrentarme con "gurús" de la seguridad de la información. Y hete aquí que encontré sapiencia y sencillez. Por suerte, aquella denuncia dio lugar a una sencilla investigación con final feliz. Pero lo más importante fue el camino abierto. Desde entonces nos hemos reunido varias veces, hemos coincidido en encuentros o jornadas, algunas organizadas por nosotros, sigo leyendo y aprendiendo de vuestro Una-al-día y los boletines mensuales sobre fraude bancario, hemos investigado juntos y, sobre todo, lo más importante, cuando os hemos llamado, allí estabais.

Ya habéis visto que yo soy pedigüeño por naturaleza. Para ser más claros, que no me corto a la hora de pedir. Pido apoyo para el Grupo de Delitos Telemáticos, para su trabajo. Somos pocos y nuestro saber es limitado. Somos Guardias Civiles, investigadores formados en el campo de la informática, y no informáticos formados en el campo de la investigación. Y eso tiene sus contrapartidas. Nuestras limitaciones técnicas. Y contra eso, siguiendo el consejo de mi antecesor, no tenemos otra solución que apoyarnos en los amigos, en gente como vosotros.

H: ¿Cuáles han sido vuestros éxitos más importantes?

JS: Relacionados con los delitos y al margen de la pornografía infantil, recuerdo éxitos como por ejemplo:

En 2003, la operación Piolín. Identificación y detención de una persona que tras la instalación de programas del tipo troyano, obtuvo contraseñas ajenas para acceder al servicio de banca electrónica. Una vez en su poder, realizó distintas transferencias bancarias hasta paraísos fiscales.

En 2003, la operación Ronnie. Esclarecimiento del mayor ataque documentado de Denegación de Servicios Distribuidos (DDoS) a distintos servidores de Internet, que afectó a más del 30% de los internautas españoles y a varios de los proveedores de Internet más importantes de España.

En 2003 también, la operación Clon. Detención de una persona presuntamente implicada en la creación y difusión de un virus informático (tipo troyano) que podría haber afectado a más de 100.000 usuarios de Internet en lengua castellana. Se trata del famoso "cabronator".

Ya en 2005, la operación Pampa. Desarticulación de una red internacional de delincuentes dedicados al fraude del "phishing", cuyo responsable se ubicaba en Argentina, logrando la colaboración internacional.

H: ¿Cómo ves el futuro?

JS: Sabéis, al igual que yo, que el escenario de la delincuencia informática es cada vez más complejo, y que ha dejado de ser un problema de la administración para ser un problema de todos. Aquellos que tenéis un papel importante en esta sociedad de la información, tenéis un compromiso social para con ella. Debemos arrimar el hombro para lograr un Internet más seguro. Por eso, estoy seguro que con lo insistente que soy, probablemente, en algún momento, podéis haber pensado que hacíais esto o lo otro para el pesado de Juan, o para los del Grupo de Delitos Telemáticos. Por eso quiero reivindicar que Hispasec, desde su esfuerzo de informarnos y ponernos al día frente a los problemas de seguridad, y desde el apoyo que ha prestado numerosas veces al Grupo de Delitos Telemáticos de la Guardia Civil, no ha hecho más que asumir ese compromiso de responsabilidad social. Como representante de una unidad policial comprometida directamente con la seguridad de la sociedad de la información, gracias, y como destinatario muchas veces directo de esa ayuda, mil gracias más. Y por favor, no abandonéis el camino. Sin vosotros nos sentiríamos más inseguros. Se me olvidaba, ¡Felicidades Una-al-día! Por el bien de todos, que cumplas muchos más.



Capítulo

3

AÑO 2001

7D1

3721

11111010001



978307200 – 1009843199



Durante este año...

_ Alguien celebró la llegada del 2001 instalando durante la noche un **monolito** de casi tres metros de alto en Washington's Magnuson Park de Seattle, en clara referencia a 2001: Una odisea en el espacio. El objeto desapareció tan misteriosamente como vino.

_ El 15 de enero nace la **Wikipedia**. Un instrumento que marcaría el inicio de la Internet colaborativa. El 20 de mayo se inauguraría su versión en español.

_ La una-al-día del 21 de enero, "Un gusano muy activo afecta a sistemas Linux de todo el mundo" es **la primera noticia firmada criptográficamente**. Con esto se validaría a partir de entonces la integridad y procedencia de la información.

_ **Javier Bardem** se convierte en el primer actor español candidato a los premios Oscar por su interpretación en la película de Julian Schnabel "Antes que anochezca". Lo ganaría finalmente en 2008 por su papel en "No es país para viejos" de los hermanos Cohen.

_ El agente del FBI **Robert Hanssen** es arrestado por cargos de agente doble que había proporcionado información para Rusia durante veinte años. Hanssen, que era agente del FBI desde 1976, fue arrestado en febrero de 2001 acusado de vender secretos a la inteligencia rusa por valor de 1.4 milllones de dólares y por diamantes. Había sido doble agente por 22 años. El 6 de julio sería declarado culpable por espionaje. Se trata del caso de doble agente más escandaloso de todos los tiempos. Sus actividades son calificadas como "el mayor desastre de la inteligencia americana en la historia". Actualmente cumple cadena perpetua sin posibilidad de libertad condicional en Colorado.

_ A Robert Tools se le instala un **corazón completamente artificial** por primera vez el 2 de julio. El artefacto se alimentaba de una batería recargable y se llamaba AbioCor. Tools vivió 151 días con el implante. Posteriormente se harían muchos otros trasplantes con éxito, alargando sustancialmente la vida de los pacientes.

_ El 20 de julio muere **Carlo Giuliani en las protestas por la cumbre del G-8**. Giuliani era un activista antiglobalización italiano que fue disparado por la policía italiana en Génova durante la reunión del G-8. Su muerte, sobre la que se celebró un juicio en el que no se condenó a nadie, lo convertiría en un símbolo de la lucha antiglobalización y del compromiso. Sería homenajeado en numerosos actos e incluso canciones. Los violentos incidentes se sucederían con más virulencia en posteriores reuniones de este grupo de los ocho países más poderosos del mundo. Los protestantes acusaban de injusto el hecho de que sólo ocho países decidieran por todo un plantea por el simple hecho de ser los más poderosos.

_ El 1 de agosto comienza a desaparecer de las gasolineras la **gasolina Super**, la única con plomo.

11 de septiembre. El mayor atentado terrorista de la historia. Se ataca simultaneamente a las Torres Gemelas en Nueva York y a El Pentágono en Washington DC. Extremistas islámicos secuestran varios aviones comerciales y los estrellan durante la mañana contra unas abarrotadas torres, donde mueren más de 3000 personas. En España se recibe la



noticia en directo durante los informativos de la tarde, que no se detiene en ninguna cadena según avanza la información hasta enlazar con los de la noche. Se reciben primero las imágenes de una de las torres ardiendo, existe mucha confusión. Minutos más tarde se asiste en directo a la colisión del avión comercial con la segunda torre. Ambas se vienen abajo durante la tarde, entre humo, llamas e impactantes imágenes de sombras cayendo desde las ventanas. La página web de la CNN, completamente saturada a visitas mientras se producen los atentados, debe aligerar la web de todo contenido superfluo para que cargue más rápidamente ante la importante demanda. La red Al Qaeda y su líder Osama bin Laden, se atribuirían la autoría de los ataques. La seguridad a todos los niveles se convertiría en el asunto prioritario para gobiernos, instituciones y empresas privadas. El mundo parece mucho más vulnerable, se desafía el poder del país más poderoso. Nada vuelve a ser igual, comienza la lucha a gran escala contra el terrorismo mundial.

Poco después de los ataques a las Torres Gemelas, se detectan los primeras cartas que contienen antrhax, dirigidas a las redacciones de noticias de las norteamericanas ABC News, CBS News, NBC News, el New York Post y el National Enquirer. Morirían dos personas y otras 17 se infectarían.

_ En septiembre, Google obtiene la patente de su **PageRank**, el algoritmo de búsqueda de su motor, el corazón de su éxito. En febrero había comprado Deja News (archivo de grupos Usenet), comenzando así un largo historial de adquisiciones empresariales.

_ Se difunde en spam y por importantes medios de comunicación el bulo de **Nostradamus**. Una falsa profecía atribuida a Nostradamus, en la que supuestamente predice el ataque a Estados Unidos y el comienzo de la tercera guerra mundial. Reputados periodistas se hacen eco de la cita sin constatar su veracidad, aun contando con un error garrafal. Está datada en 1654 y Nostradamus murió en 1566. Se difunden varias versiones. Hace referencia a una supuesta predicción de Nostradamus en 1654 donde se anuncia que la tercera guerra mundial comenzará con la caída de “dos hermanos”, imagen que recuerda a la destrucción de las torres gemelas del World Trade Center. Otras versiones del hoax van aún más lejos, incluyendo referencias a los “pájaros de hierro” o indicando el día y mes del suceso. Otro bulo muy popular corresponde al número de vuelo de los aviones implicados en el ataque. Se difunde por email que uno de sus **códigos de vuelo** es Q33NY, que codificado con el tipo de letra Wingdings resulta en ✈▯▯☠✡. Muchos, tras comprobar que es cierto, lo toman como una profecía, cuando en realidad el número no corresponde a ningún avión estrellado.



_ Nintendo lanza **GameCube**. La consola más pequeña (y barata) del momento. Cuesta unos 200 dólares. Su CPU corre a 485 Mhz y cuenta con 24 megas de RAM.

_ El 7 de octubre empieza la invasión de **Afganistán por parte de Estados Unidos** y sus aliados.

_ En octubre aparecen casi simultanemamte el primer **iPod** y Windows XP. El primer iPod (que luego pasaría a llamarse iPod Classic) venía con la rueda mecánica, no con la táctil que le haría popular dos años después. Su capacidad es de 5.10 gigas y aguanta sólo 10 horas de audio. El primero con la pantalla en color se fabricaría en 2004. En 2007, la versión más avanzada de iPod, el iPod Touch, sería completamente táctil, y su batería soportaría 22 horas de audio y hasta 32 gigabytes de capacidad. Supuso una revolución en el mercado de los dispositivos de audio portátiles, y ha resultado uno de los productos de más éxito para Apple.

Nace **Windows XP**, el que sería el sistema operativo más exitoso de Microsoft hasta la fecha. Es heredero directo de la filosofía NT y Windows 2000, arrastrando por fin para el entorno doméstico una buen parte de sus mejoras con respecto a la seguridad. Trivialidades como el fondo de pantalla, el aspecto casi infantil, la necesidad de "activar" el producto (una apuesta por la eliminación de la piratería) incomoda a sus detractores. XP supone una ruptura con la filosofía anterior de los Windows 9x y Me, en los que no existía posibilidad de asegurar el sistema. XP es multiusuario, soporta NTFS, cifrado de datos, los servicios se ejecutan bajo cuentas más limitadas, las contraseñas nulas no permiten a usuarios externos entrar por la red, mejoras en la gestión de versiones de librerías, se introduce Authenticode... sin embargo son pocos los que aprovechan estas ventajas y utilizan el sistema en permanente modo administrador, heredando los problemas de seguridad de sus predecesores. XP mejoraría de forma sustancial con el Service Pack 2 en 2004, tanto en seguridad como estabilidad. Paradójicamente y a pesar de su rechazo inicial, se convertiría en el principal problema para la propia Microsoft cuando intentara introducir en 2007 su nuevo sistema operativo Windows Vista. XP se mantiene en el mercado 6 años, mucho más de lo que en un principio se esperaba (Vista debía estar listo para 2004-2005) y los usuarios (y el malware) se resistirían a abandonarlo.

_ Se producen los **cacerolazos argentinos**. Forman parte de un estallido popular que causa, entre otros efectos, la renuncia del presidente Fernando de la Rúa, ante una agudísima recesión económica. Argentiza alcanza entre 2001 y 2002 cifras récord de pobreza (53%) y de paro (20%). Se producen saqueos a tiendas y supermercados y se declara el estado de sitio en todo el país. Renuncia el ministro de economía de Argentina Domingo Cavallo, el presidente y las revueltas se saldan con alrededor de 20 manifestantes muertos.

_ India se convierte en la segunda nación en rebasar los **mil millones de habitantes**. La primera fue China en 1979.

Seguridad Informática



_ En enero se descubre **Ramen**, un gusano para Linux bastante activo. Afecta a sistemas RedHat 6.2 y RedHat 7.0 aprovechándose de vulnerabilidades conocidas (y con parches) en los servicios rpc, wuftp o LPRng. En abril se detectaría también un nuevo gusano, llamado Adore, que aprovechándose de las vulnerabilidades de seguridad de los sistemas operativos de software libre infectaría a sistemas Linux.

_ **Hotmail** presenta graves deficiencias en la detección de virus. McAfee, el motor antivirus con que cuenta el sistema de webmail de Microsoft, llevaba 6 meses sin actualizar sus firmas. Cientos de muestras de malware quedan potencialmente indetectadas. McAfee culpa a Microsoft de no mostrar interés en la actualización. La relación entre el antivirus y Hotmail se va degradando hasta que a finales de 2004, Microsoft optaría por usar Trend Micro en Hotmail, y prescindir de McAfee.

_ En febrero de 2001, **Hispasec inaugura su nuevo servicio de detección de virus on-line** gracias a un acuerdo con la firma antivirus Trend Micro. Este nuevo servicio gratuito permite realizar el análisis, la detección y la desinfección de los virus directamente desde una página web. Se accede a través de la dirección http://www.hispasec.com/housecall. Se visualizará una ventana con el árbol de directorios de las unidades del sistema del usuario, momento en que se pueden seleccionar las unidades o directorios que se desean analizar.



_ El famoso gusano **Anna Kournikova** se propaga por correo en los Windows de todo el mundo. Camuflado como una foto de la conocida tenista Anna Kournikova, promete enseñarla desnuda. Miles de usuarios no dudan en ejecutar el archivo y quedan así infectados. Tiene varios alias, I-Worm/Lee.O o KALAMAR. Se vale de Outlook y Outlook Express para reproducirse. El mensaje incluye un archivo adjunto, con el nombre "AnnaKournikova.jpg.vbs", que dependiendo de la configuración del sistema podrá aparecer únicamente como una imagen jpg, lo que confunde a los usuarios para que abran la falsa imagen. Es considerado una mancha en el expediente de detección de antivirus, puesto que fue "programado" con una herramienta de creación vírica conocida, a golpe de ratón, con lo que su detección debía resultar teóricamente sencilla, y desde luego, a tenor de los niveles de infección que consiguió, no fue así.

En febrero **Phil Zimmerman abandona NAi**. En un mensaje dirigido a todos los usuarios de PGP el mítico Phil Zimmerman (creador y desarrollador del extendido programa de cifrado PGP, considerado un luchador por las libertades al desafiar las leyes de exportación de material cirptográfico de Estados Unidos) anuncia su marcha de Network Associates. El mensaje de Zimmerman comienza recordando la compra de PGP Inc. por NAi a finales de 1997. Durante esos tres años Phil permanece en la compañía para proporcionar orientación técnica para el desarrollo de PGP y asegurar la integridad criptográfica del producto. Pero anuncia que la visión del futuro de PGP que tiene NAi difiere de la suya por lo que decide cambiar a otros proyectos más acordes con sus objetivos de proteger la privacidad de las personas. Hasta la versión 6.5.8 la seguridad quedaba garantizada en PGP con la publicación completa del código fuente. Pero la entrada de un nuevo administrador en la división PGP Security a finales del 2000 cambiaría el rumbo marcado hasta el momento, con su decisión de reducir la cantidad de código publicado. A pesar de ello, Phil garantiza que el desarrollo se ha mantenido bajo su control y se encuentra libre de puertas traseras. Zimmerman anunciaría su paso a Hush Communications, desarrolladores de HushMail para ayudarles en la implementación del estándar OpenPGP en sus desarrollos futuros. De igual forma también colaborará con Veridis para la creación de nuevos productos OpenPGP, incluido software para autoridades certificadoras.

_ Aparece **Winux**, primer virus para ejecutables de Windows y Linux. Aunque no se detectarían casos de infecciones significativas. Se trata de una prueba de concepto. También conocido como Lindose, es un virus escrito en ensamblador que infecta ejecutables Windows (PE) y Linux (ELF) por acción directa

(no queda residente en memoria). Su única acción consiste en buscar ficheros con estos formatos en el directorio actual y superiores en el caso de Windows, para proceder a su infección. No posee ningún tipo de efecto destructivo. En el interior del virus se puede encontrar una cadena con el apodo del autor, Benny, y con referencias a 29A, el famoso grupo de creadores de virus conocido por sus innovaciones en la escena vírica.

_ **VeriSign**, la empresa líder en emisión de certificados para Internet, protagoniza en marzo uno de los **fiascos** más importantes de su historia que compromete de lleno la seguridad de los usuarios de Windows. Emiten dos certificados a un impostor que se hizo pasar por trabajador de Microsoft. Esto permitiría firmar virus y cualquier software malicioso como si fueran aplicaciones originales de Microsoft. A efectos prácticos y en líneas generales, el trabajo de VeriSign (raíz del problema) consiste en hacer las veces de notario mediante la emisión de certificados digitales (autoridad de certificación). Las empresas que quieren certificar la autenticidad de sus aplicaciones ante los usuarios solicitan a VeriSign un certificado con el que firmar digitalmente su código. Además de exigir el pago correspondiente, VeriSign tiene un protocolo para verificar la identidad del solicitante, es decir, la empresa o persona con los privilegios adecuados a nombre de la que se emite el certificado. El protocolo falla y los certificados pasan por válidos. McAfee y Symantec saltan a la arena para anunciar que sus antivirus cuentan con actualizaciones para detectar los certificados fraudulentos, como si de un virus se tratara. Los certificados serían revocados en una posterior actualización de Microsoft. Todavía pueden ser vistos en el respositorios de certificados revocados de muchos Windows XP.

_ Se publica la primera metodología de libre uso para la verificación de la seguridad. **OSSTMM (Open Source Security Testing Methodology Manual)**. Se trata de un manual dirigido a la comunidad profesional dedicada a la seguridad informática, que describe el conjunto mínimo de pruebas que deben realizarse en un test de intrusión, "hacking ético" y análisis de la seguridad de la información. El objetivo es ofrecer un marco estandarizado para la realización de las valoraciones de seguridad.

Para el desarrollo del manual se han tenido presente diversas normativas legales (entre las que se incluye la ley española de protección de datos), de forma que también puede ser utilizada en la evaluación del cumplimiento de las mismas. Se trata de un proyecto abierto, distribuido bajo licencia GNU. Se distribuye en inglés y en formato HTML, PDF y PS. En su primera época, el **Open-Source Security Testing Methodology Manual** se aloja en el mítico dominio http://www.ideahamster.org. El proyecto Ideahamster publicaría también en octubre de ese mismo año un manual con una metodología para la programación segura de aplicaciones para Internet. La metodología para la programación segura es un suplemento de la metodología de seguridad OSSTMM.

_ Se descubre en mayo **W32/Hello**, primer gusano que se distribuye por MSN Messenger e infecta a máquinas Windows.

_ En mayo, y tras varios meses desde su descubrimiento, **Magistr** sigue activo y el número de infecciones sigue aumentando. El polimorfismo de este virus hace mella en algunas soluciones antivirus. La ingeniería social utilizada por el autor del espécimen y el descuido de los usuarios hace el resto. Magistr contiene rutinas para borrar los discos duros, la CMOS y la Flash BIOS. Tendría más versiones.

Aunque lleva muchos meses circulando, el **bulo del archivo Sulfnbk.exe** se vuelve tremendamente popular. El archivo está presente en todos los Windows 98 y Me del



momento, y corresponde a una aplicación legítima del sistema. A través del correo los propios usuarios reenvían constantemente una alerta que indica que quien posea ese archivo en su sistema, está infectado por un virus. Los usuarios reciben un mensaje donde se advierte de un supuesto nuevo virus y facilita además unos sencillos pasos para poder comprobar si estamos infectados. El método consiste en buscar el fichero sulfnbk.exe en el sistema, y eliminarlo en caso de encontrarlo pues supondría una infección. No son pocos los que reaccionaban con pánico ante la supuesta evidencia de un virus en su sistema. Algunos formateaban completamente el disco duro. Lógicamente, al comprobar que están infectados y que las intrucciones son precisas, alertan a sus amigos por email y la cadena se realimenta. Afortunadamente, el impacto es mínimo. Se trata de una utilidad de Windows que permite salvar y restaurar los nombres largos de los ficheros si han sido reemplazados por el formato corto compatible con MS-DOS. Poco después el bulo **se repetiría con el archivo jdbgmgr.exe,** cuyo icono correspondía a un osito de peluche. Se baraja la posibilidad de que el origen del bulo no sea intencionado, algunas hipótesis apuntan a que alguien recibió un mensaje donde se adjuntaba el fichero sulfnbk.exe infectado con el gusano Magistr. El antivirus del usuario pudo alertarlo, e interpretó que existía un gusano que se distribuía con este nombre de fichero, de ahí que comenzara a alertar a sus contactos más próximos.

_ El gusano **sadmind/IIS**, que aprovecha vulnerabilidades ya conocidas y parcheadas para reproducirse y modificar páginas web, afecta a versiones sin actualizar de Microsoft IIS y de Solaris hasta Solaris 7 (incluida). Este gusano explota una vulnerabilidad en los sistemas Solaris para posteriormente instalar un software capaz de atacar servidores web con Microsoft Internet Information Server.

_ En verano Microsoft anuncia que no publicará el **Service Pack 7** para el sistema operativo Windows NT.

_ **Hispasec Sistemas y el Instituto para la Seguridad en Internet (ISI)** comienzan a organizar cursos presenciales, eminentemente prácticos, dirigidos a todos aquellos administradores de sistemas y desarrolladores de entornos Microsoft.

_ **La Agencia de Seguridad Nacional de los Estados Unidos** pone a disposición de los usuarios de Windows 2000 una serie de directrices con el fin de facilitar una mejor administración del sistema operativo de Microsoft. La documentación liberada consta de 5 plantillas para usar con el editor de configuración de seguridad, más otras 17 plantillas que cubren diversos aspectos sobre la seguridad en sistemas operativos y tres documentos que tratan fundamentalmente sobre seguridad en paquetes de software populares relacionados con Windows 2000.

_ **En junio Hispasec proporciona un test** mediante el que los usuarios podrán simular la llegada de un virus a su sistema a través del correo electrónico. De esta manera, se podrá comprobar la reacción del programa antivirus instalado en el ordenador. El test consiste en enviar un mensaje con el archivo EICAR como documento adjunto a la dirección de correo electrónico del usuario y comprobar la reacción del antivirus a su llegada.

_ Aunque todavía no son muy usadas, en julio IBM presenta una herramienta de seguridad para redes inalámbricas. Se trata de la primera herramienta existente para la realización de auditorías y recopilación

de información relacionada con la seguridad, de forma automática, en las redes inalámbricas 802.11. **Wireless Security Auditor** es el prototipo de una aplicación que funciona en Linux y permite a los administradores de red la localización de la existencia de puntos de acceso vulnerables y evitar que supongan una amenaza para la seguridad. En esos momentos solo se disponen de dos mecanismos de seguridad existentes para las redes inalámbricas 802.11: una técnica de cifrado denominada Wired Equivalent Privacy (WEP) y un algoritmo de autenticación denominado Shared Key Authentication. Tanto WEP como Shared Key son opcionales y habitualmente los puntos de conexión de las redes inalámbricas son distribuidos con ambas funciones desactivadas. Poco después se demostraría que el WEP era un cifrado débil e inútil.

_ En verano aparece **SirCam** un gusano de propagación masiva. Viaja adjunto en un e-mail con las cadenas “Hola como estas ?” y “Nos vemos pronto, gracias” como primera y última línea del cuerpo del mensaje. Este gusano consigue una especial relevancia en países de habla hispana, sin duda gracias a la utilización de frases en español, además del inglés, para formar los mensajes en los que se adjunta.



_ Es un verano negro en cuestión de virus de propagación masiva. Aparece también **Code Red**. Ataca a los servidores IIS no actualizados. En los tres primeros días después de su descubrimiento, ya se contabilizan más de cinco mil servidores infectados. Para atacar los servidores utiliza el desbordamiento de búfer existente en el filtro ISAPI de Microsoft Indexing Service. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el servidor con privilegios de SYSTEM, lo que le facilita un control absoluto de la máquina. Las páginas web en los servidores infectados son reemplazadas por un reconocible texto que perduraría en muchos servidores durante años.

_ En agosto aparecería el gusano **“Code Red II”**. El parecido con la versión original es el mecanismo de propagación. Una de las características de esta nueva mutación es el abrir diversas puertas traseras en la máquina infectada.

_ En agosto Hispasec descubre **OUTLOOK.PDFWorm**, el primer gusano que se presenta en un archivo PDF (Portable Document Format). No es la única novedad: este espécimen se distribuye utilizando funciones de Outlook nunca vistas antes en un gusano. Aunque es un virus de laboratorio que apenas ve la luz, se trata de una importante semilla que puede hacer proliferar este tipo de virus insertados en archivos PDF, un formato hasta ahora considerado seguro por los usuarios.

_ Microsoft presenta **HFNETCHK** una utilidad para los administradores de Windows que permite determinar la presencia o ausencia de las diferentes actualizaciones de seguridad en uno o varios ordenadores. Sería el germen de lo que posteriormente se conocería como Microsoft Baseline Security Analyzer.

_ En septiembre, la comisión de la Unión Europea encargada de determinar la existencia real de **Echelon**, entrega su informe que indica la existencia de la red de espionaje. Tras las denuncias de importantes compañías europeas, testimonios de ex-operarios de la red y rumores más que fundados, el parlamento europeo decidió fundar en 2000 una comisión para determinar la existencia o no de Echelon, así como la participación del Reino Unido en ella. El informe realiza reveladoras aseveraciones: Echelon existe y la privacidad es un derecho fundamental. También recomienda el uso de comunicaciones cifradas, a todos los niveles. Se llega incluso a afirmar la conveniencia de desarrollar campañas de concienciación institucionales.

_ En septiembre, **nimda** campa a sus anchas por los sistemas Windows. Llega adjunto en un mensaje con el nombre de archivo "readme.exe", o intenta descargarse al visitar la página web de un servidor infectado. Su enorme capacidad de propagación se debe a que infecta y se difunde aprovechando tanto las infecciones entre clientes (módulo readme.exe) cómo a través de servidores Web basados en Internet Information Server (módulo Admin.dll). Entre otras características también destaca la compartición de la unidad C: en los sistemas infectados. A grandes rasgos, nimda suma características de SirCam y Code Red.

_ Virus de poca monta como **WTC.EXE**, alias "Vote", nunca habrían saltado desde algunas casas antivirus a los medios de no ser por las referencias al World Trade Center. Aunque sus efectos dañinos son muy anunciados, no se esperan infecciones significativas. "Vote" se covierte en objeto de discordia entre las propias casas antivirus. Mientras que algunas lo situan en las primeras horas como "In the wild" (distribución generalizada), otras lo catalogan como un "hype" (exageración).

_ Microsoft publica un polémico llamamiento a la comunidad profesional dedicada a la seguridad para que **no se divulguen los errores detectados en sus productos**. El objetivo de la compañía es "no proporcionar información gratuita a los hackers para explotar las debilidades del sistema". En un comunicado firmado por Scott Culp, responsable del Microsoft Security Response Center se atribuye a la "anarquía informativa" existente en la actualidad el éxito alcanzado por los últimos gusanos: Code Red, Lion, Sadmin y Nimda. Microsoft alega: "Si bien la industria debe esforzarse en producir productos más seguros, no es realista esperar que seamos capaces nunca de alcanzar la perfección. Todos los programas no triviales contienen bugs y los sistemas operativos modernos son cualquier cosa excepto triviales. De hecho, se pueden incluir entre las cosas más complejas que nunca haya realizado la humanidad. Las vulnerabilidades de seguridad están aquí para quedarse".



_ Sony solicita a un programador experto que retire de Internet sus programas gratuitos para modificar los comportamientos y añadir nuevas funcionalidades al perro-robot **Aibo**. La decisión de Sony provoca protestas en la comunidad de seguidores de Aibo que comienzan a retirar sus páginas webs dedicadas a esta cibermascota, además de recomendar a los usuarios que dejen de comprarlo.

_ Las actualizaciones de seguridad específicas para los sistemas operativos de Microsoft en español ya no tienen que esperar tanto. A final de año parece que Microsoft presenta mejoría en este aspecto. El Service Pack 2 para Internet Explorer 5.5 **versión en español tiene un retraso de sólo 10 días** respecto a la versión de Estados Unidos, mientras que el Service Pack 1 para SQL Server 2000 apenas los separan 3 días, todo un récord en comparación con las semanas, incluso meses, de tiempos atrás.



_ En noviembre Hipasec lanza SANA. El Servicio de Análisis, Notificación y Alertas (SANA) es un completo sistema de información en tiempo real destinado a cubrir las necesidades de empresas y profesionales en materia de seguridad informática. SANA hace llegar la información más reciente que pueda afectar o ser de interés para el usuario, según el perfil que haya configurado. Utiliza distintos formatos de notificación, a través del correo electrónico y mediante mensajes SMS a teléfonos móviles, un servicio de alertas que trabaja 24 horas al día, 365 días al año y que sigue vigente.

_ En noviembre aparece **BadTrans**, que también tendría varias versiones. Se distribuye por correo electrónico y es capaz de ejecutarse de forma automática en Outlook y Outlook Express con tan sólo visualizar un mensaje infectado. "BadTrans.B" explota una vulnerabilidad conocida de Internet Explorer que permite la ejecución automática de un binario adjunto en un mensaje de correo (.EML). Para

lograrlo modifica la cabecera MIME que hace referencia al archivo de forma que simula ser un formato confiable. Esto provoca que Internet Explorer lo abra sin preguntar al usuario.

_ Nace **Passport .NET** (que posteriormente sería Live), un servicio en línea que hace posible que pueda utilizar una dirección de correo electrónico y una única contraseña para iniciar una sesión de forma segura en cualquier servicio o sitio web participante de Passport.

_ En diciembre Hispasec desarrolla una solución para los timos basados en números de tarificación adicional 906. En el contexto de la Campaña Nacional de Seguridad en la Red, inciada por la Asociación de Internautas, Hispasec presenta el desarrollo de **CheckDialer**, una solución contra el llamado "fraude 906". Cada día aumentan los sitios webs que anuncian el acceso a contenidos pornográficos de forma gratuita, sin necesidad de realizar pagos con tarjeta de crédito. Muchas de estas ofertas sólo piden al usuario que descargue e instale un programa gratuito que le permitirá disfrutar de los contenidos. La mayoría de los usuarios, bien arrastrados por publicidad engañosa, bien por no leer la letra pequeña que se esconde en estos programas, desconocen que en realidad están utilizando marcadores o "dialers" que conectan a través de números 906 de tarificación especial en España, en el mejor de los casos a 100 pesetas (0, 60 euros) el minuto. CheckDialer, es un programa para sistemas Windows que monitoriza las conexiones que se realizan a través de un módem (o RDSI). Su éxito perduraría hasta nuestros días, en países en los que aún es habitual la conexión por módem.

_ El servicio UPNP **(Universal Plug and Play)** sufre de una grave vulnerabilidad en Windows XP que permite la ejecución remota de código. Aunque no sería aprovechada de forma masiva, un error muy parecido sentaría las bases para la nefasta propagación de Blaster y Sasser dos años después. El servicio UPNP (Universal Plug and Play) es una ampliación del ya conocido Plug and Play. Mientras que este último permite que Windows reconozca los dispositivos que están instalados directamente a nuestro ordenador, UPNP amplía esta funcionalidad a las redes TCP/IP.

Una al día

13/02/2001 AnnaKournikova: ¿fracaso de la comunidad antivirus?

El último virus de gran propagación, alias "AnnaKournikova", pone en entredicho la utilidad de muchas de las soluciones antivirus existentes en el mercado. El virus es el resultado de usar un kit de creación automática, que permite diseñar gusanos sin necesidad de saber programar y que se conoce desde agosto de 2000. Para colmo se ha contado con la "colaboración ciudadana", ya que son muchos los usuarios que se han dejado engañar por prácticamente un "remake" del archiconocido "ILOVEYOU". A bote pronto se pueden sacar algunas conclusiones de este último brote vírico de escala mundial:

* La tan anunciada detección heurística en las soluciones antivirus parece que queda en la mayoría de los casos en simple publicidad, a juzgar por la propagación que ha conseguido alcanzar este gusano.

"AnnaKournikova" está creado con "Vbs Worms Generator", un kit de creación automática desarrollado por un argentino apodado [K]Alamar, que permite diseñar gusanos a golpe de ratón con tan sólo seleccionar ciertas características en un menú de configuración.

Según las últimas noticias, fue un joven holandés quién generó el "AnnaKournikova" aprovechando esta

utilidad. El autor es lo de menos, lo peor es que provocar un caos mundial está al alcance de cualquiera que sepa manejar Windows. En estos momentos tenemos que "agradecer" que el joven no pulsara en la opción de payload (efecto) dañino, ya que a juzgar por la propagación alcanzada hubiera causado perdidas multimillonarias entre empresas y usuarios.

Esta utilidad está disponible en Internet desde agosto del año pasado y, como es normal, todos los gusanos generados tienen mucho código en común, lo que hace trivial que se pueda detectar cualquier versión que produzca. En el caso concreto de "AnnaKournikova", el algoritmo de descrifrado que puede verse a simple vista es exactamente el mismo, línea por línea, que el de gusanos reconocidos hace meses, con la única diferencia en el nombre de las variables. No se entiende pues que este gusano haya podido infectar sistemas que contaran con un antivirus, a no ser que la má simple de las heurísticas brille por su ausencia en dichas soluciones.

A continuación, se presentan los resultados de un test llevado a cabo por Hispasec en relación a la eficacia de los motores antivirus en el caso del gusano "AnnaKournikova", según poder de detección/heurística antes de que éste saliera a la luz. En el grupo de los aprobados se encuentran los antivirus que detectaron el virus desde el primer momento sin necesidad de una actualización adicional.

Aprobados: AVP/Karspersky, F-Secure, McAfee, TrendMicro

Suspensos: Norman, Norton, Panda, Sophos * La ingeniería social sigue siendo la mejor arma de los virus contra los usuarios.

No ha hecho falta crear ninguna nueva técnica de infección, aprovechar agujeros de seguridad, ni desarrollar complicadas rutinas. Si con "ILOVEYOU" no se pudo resistir la tentación de leer una declaración de amor, en esta ocasión ha bastado con el simple reclamo de ver una foto de la joven tenista Kournikova. Los encantos de Anna hicieron olvidar a miles de usuarios la regla básica: no abrir archivos adjuntos no solicitados.

* El actual esquema de detección de virus que implementan la inmensa mayoría de las soluciones antivirus no es efectivo ante virus nuevos que aprovechan Internet como canal de propagación.

Primero es necesario que el virus nuevo infecte a algunos usuarios, que éstos se percaten y envíen una muestra al laboratorio antivirus. Allí analizan el espécimen y desarrollan una vacuna que ponen a disposición del resto de sus usuarios registrados a través del proceso de actualización.

Siempre existen unos usuarios perjudicados que reciben el primer azote del virus (tengan sus antivirus actualizados o no), y el resto de la comunidad se encuentra indefensa mientras que se desarrolla la vacuna específica y, posteriormente, actualizan su antivirus.

Este esquema podía ser válido hace años, cuando los virus se propagaban con el intercambio de disquetes. Hoy día, en cuestión de horas (las que se tardan en el mejor de los casos en analizar y proporcionar una vacuna específica), un gusano puede haber causado cientos de miles de infecciones aprovechando la infraestructura de Internet. La Red ha facilitado las actualizaciones de los productos, pero aun se muestra más efectiva como canal de distribución de una nueva generación de virus. Es la pescadilla que se muerde la cola.

Sin duda es un esquema productivo para las casas antivirus, que se aseguran el mantenimiento de por vida gracias a la necesidad de actualizaciones continuas, y útil para el usuario si no tiene la desgracia

de sufrir la infección en los primeros momentos. En cualquier caso, no es una solución óptima y ya hay movimientos en pro de esquemas que ataquen el problema del código malicioso de raíz, de una forma más global y genérica.

Bernardo Quintero

15/04/2001 Windows XP, ¿el final de los virus informáticos?

Este artículo forma parte de los contenidos de la Comparativa Antivirus 2001, en él se incluyen los comentarios de Eugene Kaspersky y Mikel Urizarbarrena, presidentes de AVP y Panda Software respectivamente, así como de "Zulu", el creador de virus-scripts más destacado de los últimos tiempos. Junto a ellos analizamos las nuevas características de seguridad que Windows XP puede incorporar en un intento de frenar la actividad de los virus informáticos.

A finales de noviembre, un portavoz de Microsoft, Jim Ewel, dejaba entrever en una conferencia en Londres algunas de las nuevas características que Windows XP, por aquel entonces conocido como Whistler, incorporaría en materia de seguridad. El anuncio de que Whistler podría bloquear cualquier aplicación que no contara con un certificado digital suscitó tanto interés como polémica.

En respuesta a los problemas de los virus que utilizan el correo electrónico, Microsoft planeaba extender la nueva característica a "cada porción de código que pueda ejecutarse en la máquina"", comentó Ewel. A la espera de que Microsoft arroje más luz sobre esta funcionalidad, este anuncio ha suscitado de nuevo un debate sobre la posibilidad de crear un entorno seguro contra virus informáticos.

Para comprender mejor en qué consistiría esta característica, basta con conocer el modelo de seguridad en el que se basan los controles ActiveX. Estos componentes en su aplicación en Internet son muy similares en aspecto a los applets de Java, ya que pueden formar parte de cualquier página web, con el peligro potencial que eso podría acarrear.

Microsoft, a diferencia de Sun cuando desarrolló Java, no limitó en ningún momento la capacidad de estos controles. Un ActiveX puede llevar a cabo cualquier tipo de acción en el sistema, si bien siempre debe estar convenientemente identificado con un certificado digital que proporcione información sobre quién lo ha desarrollado. Si el desarrollador es fiable, el sistema lo ejecuta directamente, si no lo es o carece de certificado, el sistema informa al usuario que es él quien decide en última instancia si desea ejecutarlo o no. Un sistema sencillo y que deja finalmente la patata caliente al usuario, pero que se muestra efectivo apenas se aplique algo de sentido común.

El anuncio de Microsoft en relación a Windows XP extendería esta filosofía a todo el sistema operativo. Es decir, podríamos configurar un entorno donde sólo se permitiera la ejecución de las aplicaciones que vengan firmadas digitalmente por ciertos desarrolladores y negar el permiso a cualquier otro código. Esto, sin duda, representa un paso hacia una solución genérica al problema planteado por los virus informáticos y al malware en general.

A la espera de conocer más detalles sobre esta nueva característica, y ver finalmente cuál es la implantación real (y libre de fallos), parece claro que se trata de una funcionalidad que podría tener su mayor acogida en entornos corporativos. Un administrador de red podría controlar con exactitud qué software tiene permiso de ejecución en su compañía, por ejemplo aquellos códigos que vengan firmados por Microsoft o

por el propio certificado de su empresa. De esta forma, el administrador firmaría los propios desarrollos de la empresa o el software propietario que está reconocido por la compañía, y evitaría la ejecución de cualquier otra aplicación, incluido virus, programas que los usuarios se intenten bajar de Internet, etc.

Desde el punto de vista del usuario la cosa cambia bastante, ya que es un consumidor habitual de shareware y freeware. Es bastante improbable que los desarrolladores de este tipo de software paguen el registro de un certificado digital para después regalar sus aplicaciones. La experiencia también dicta que el usuario tiende a desatender las pantallas de peligro y al final opta por inhabilitar este tipo de sistemas de seguridad para ganar en comodidad. En cualquier caso, sería un buen momento para que los programadores Windows optasen por la filosofía de código abierto, solución óptima para todos.

Tanto las casas antivirus como los creadores de virus ven con bastante recelo este tipo de iniciativas, sino juzgad por los comentarios. Tal vez sea una buena señal.

La opinión de Mikel Urizarbarrena, presidente de Panda Software:

Sobre el papel, este sistema puede representar un avance significativo en el campo de la seguridad. Ninguna aplicación que no esté firmada digitalmente podrá ser ejecutada en la red, ninguna. En la práctica, está por ver la acogida que tendrá entre los administradores y los usuarios.

Es posible que inicialmente el sistema tenga una gran aceptación entre los administradores de red, pero creo que los inconvenientes que presenta acabarán por desaconsejarlo. ¿qué ocurrirá cuando estos vean que esa utilidad shareware que acaban de descubrir y que soluciona sus problemas no puede ejecutarse mientras esté el sistema activado, pues no ha sido certificada por Microsoft?

¿Qué sucederá con los pequeños fabricantes de software?, tendrán que adquirir certificados digitales con el coste adicional que conlleva o se les obligará a ser certificados por Microsoft. Si Microsoft hubiese optado en sus comienzos por un sistema como éste, seguramente sus productos no hubiesen alcanzado tanto éxito.

Además, un sistema de este tipo animará sin duda a los creadores de virus, pues si consiguiesen burlarlo introduciendo en una red este tipo un virus con firma digital, por la propia naturaleza del sistema, el virus correría a sus anchas por todos los ordenadores de la red. Los usuarios lo ejecutarían sin ningún temor creyéndose protegidos.

El efecto de este sistema de certificados podría compararse a desconectar un ordenador de la red y quitarle las disqueteras y CDs. El ordenador en este caso estará completamente protegido de virus,
pero, ¿seguirá resultándonos útil?

La opinión de Eugene Kaspersky, presidente de Kaspersky AntiVirus (AVP)

En los sistemas modernos hay demasiados tipos de ficheros ejecutables, programas que pueden acceder a los componentes del ordenador. También es muy complicado que un sistema no tenga problemas, incluyendo agujeros de seguridad. Por todo ello, creo que los virus seguirán existiendo aunque el entorno contemple la seguridad basada en certificados digitales.

Es posible desarrollar un entorno completamente protegido por la comprobación de firmas digitales, ¡pero los usuarios no lo usarán!, porque un entorno de este tipo no es lo suficientemente amigable... demasiadas limitaciones, demasiados avisos, demasiadas preguntas.

La opinión de “Zulu”, creador de virus (LIFE_STAGES, BubbleBoy, Freelinks, etc).

Sinceramente lo veo como algo ridículo. Si esta tecnología ya fracasó con los drivers para Windows 2000, es mucho mas probable que fracase con aplicaciones, ya que existen más cantidad de aplicaciones que de drivers y un usuario normal instala más aplicaciones que drivers. ¿Acaso alguno usa controladores de NVIDIA o Via que estén firmados digitalmente?, no me parece... Uno terminada deshabilitando el warning o aceptando por costumbre el cartelito de aviso de driver no firmado digitalmente.

Mi opinión (Bernardo) independiente al respecto es bastante escéptica, no tanto por la idea, que en la teoría me parece muy útil, sino por la implementación que al final se realice de ella. Resulta bastante extraño que Microsoft, tan dada a los problemas de seguridad en sus sistemas y que ha protagonizado prácticamente dos revoluciones en el mundo de los virus (macros e Office y el compendio Outlook/VBS), pueda resolver de un día para otro un problema de esta envergadura.

Por otro lado, también me quedan bastantes dudas en el aspecto técnico y práctico de la solución, por ejemplo, cómo este esquema va a proteger la interpretación de scripts o los problemas de seguridad de terceras aplicaciones. Imaginemos que tengo AutoCAD registrado en mi Windows XP con su correspondiente certificado digital seguro y confiable, por tanto, totalmente validado en mi sistema. Sin embargo, cada vez que abra un nuevo proyecto con este programa tengo el peligro potencial de contagio, ya que es factible realizar un virus en el lenguaje de automatización de AutoCAD.

Este artículo, parte de los contenidos de la Comparativa Antivirus 2001, fue redactado antes de que se produjera el fiasco protagonizado por VeriSign con la emisión de certificados falsos a nombre de Microsoft. Tal y como anunciábamos entonces, la publicidad y el soporte a este incidente por parte de las casas antivirus podía tener una segunda lectura basada en el contenido del presente artículo.

Los certificados falsos emitidos a nombre de Microsoft podrían haber sido aprovechados para crear un virus o gusano firmado digitalmente que traspasara sin ningún tipo de problemas la seguridad de Windows XP, incluso de forma más efectiva que los actuales gusanos ya que se trataría de código confiable. No es de extrañar entonces que las casas antivirus pusieran cierto enfasis en publicitar el incidente que vendría a demostrar la debilidad de este sistema global contra el malware que amenaza con desplazar a las soluciones antivirus actuales.

Bernardo Quintero

19/04/2001 Virus y teléfonos móviles

Nueva entrega de los contenidos y entrevistas adicionales que acompañan a la comparativa antivirus 2001 desarrollada por Hispasec, publicada en el número de abril en la revista PC-Actual y próximamente en www.hispasec.com.

Durante el pasado año el tema de los virus y ataques a teléfonos móviles ha tomado un especial protagonismo. Aunque gran parte de lo que se dice corresponde a la mitología de Internet y a simples “hoaxs” (bulos) sin ningún fundamento técnico. Resulta curioso ver como algunos de estos avisos totalmente falsos, que se caracterizan por afirmar que ante la recepción de un determinado tipo de llamada el terminal podrá quedar totalmente inutilizable, saltan a medios de prensa habitual e incluso las propias operadoras los dan como ciertos en sus páginas web.

Entre los incidentes reales más destacables nos encontramos con el gusano "Timofónica", que si bien infectaba PCs tenía como payload (efecto) el envío de mensajes SMS aprovechando una pasarela de Internet.

El i-worm "Timofónica" envía mensajes a móviles (5-06-2000)

http://www.hispasec.com/unaaldia.asp?id=587

En lo que respecta a creaciones específicas para dispositivos móviles nos encontramos con varios troyanos para EPOC, el sistema operativo de 32bits diseñado por Psion.

Virus y troyanos en ordenadores de mano (3-08-2000)

http://www.hispasec.com/unaaldia.asp?id=647

Durante la entrevista con los presidentes de AVP y Panda también charlamos sobre lo que nos puede deparar esta nueva corriente de especímenes:

- Este año pasado también se ha hablado mucho de telefonía móvil en relación a los virus, sin embargo, aún es un campo que, por fortuna, no ha sido explotado. ¿Cuáles son los factores que dificultan hoy por hoy la generación de virus/gusanos para esta plataforma?

Habla Eugene Kaspersky (presidente de Kaspersky AntiVirus - AVP)

Si, tuvimos muchas consultas al respecto cuando antes del verano del pasado año descubrimos Timofónica, un virus que realizaba spam con mensajes cortos (SMS) a teléfonos móviles GSM. Aunque el efecto del virus era mandar mensajes cortos a través de Internet aprovechando una pasarela SMS de MoviStar, en realidad no podía introducir ningún tipo de código en los teléfonos móviles, y su replicación seguía basándose en los ordenadores tradicionales.

Aunque en la actualidad no existan virus 100% operativos para telefonía móvil, es de prever que hagan su aparición en breve, ya que los dispositivos de última generación no están ni mucho menos informatizados que un ordenador personal. Habrá sistemas operativos, procesadores de texto, hojas de cálculo, editores incorporados, etc., permitiendo que los usuarios creen sus propios ficheros ejecutables y que sean fácilmente intercambiables entre dispositivos sin hilos.

Por ejemplo, hoy día existe la posibilidad de crear virus para móviles basándose en los teléfonos WAP. De momento somos muy afortunados porque los creadores de virus no han podido acceder a las herramientas de desarrollo adecuadas.

¿Cómo los operadores de telefonía móvil pueden contrarrestar el ataque de un hipotético virus para WAP? De la misma forma que los virus se detectan y eliminan en el correo electrónico hoy día. Habrá programas antivirus instalados en los gateways de WAP que filtrarán constantemente el tráfico.

Habla Mikel Urizarbarrena (presidente de Panda Software)
La telefonía móvil está caracterizada por disponer de hardware variado y de capacidad limitada. Además, no existe un sistema operativo sobre el que los virus puedan ejecutarse o provocar infecciones.

A pesar de que la tecnología WAP podría ser una base sobre la que puedan proliferar los virus, se ha visto

que es muy limitado para que los virus puedan actuar hoy por hoy.

De cara al futuro, parece que el sistema i-mode puede ser una plataforma suficientemente potente y portable como para que los virus puedan proliferar. Sin embargo esto no será posible hasta que se extienda el uso de Java en estos sistemas.

Creo que la tecnología móvil es un campo muy a tener en cuenta y que en el plazo de un año puede convertirse en una nueva vía de infección. En Panda estamos investigando este campo desde hace casi un año, así que es muy posible que exista un Panda para Móviles.

Bernardo Quintero

29/07/2001 Reflexiones sobre SirCam

Dos años después de que apareciera Melissa, el gusano que pilló desprevenidos a miles de usuarios, vamos para atrás, como los cangrejos. SirCam sólo representa una nueva faceta, unas más, del mismo problema. ¿Hay soluciones?

Desde la simplicidad de Melissa o ILoveYou, pasando por especímenes mucho más elaborados y complejos como Hybris o Magistr, el problema siempre es el mismo. Por un lado, los usuarios que no se resisten a la tentación de abrir el archivo adjunto que les llega a través del correo electrónico. Por el otro, los antivirus que siguen siendo incapaces de proteger contra virus nuevos. El resultado es siempre la infección de miles de sistemas, la espera mientras las casas antivirus desarrollan la vacuna y, después, las actualizaciones que deben realizar los usuarios para reconocer el nuevo virus.

En el mejor de los casos, cuando se trata de gusanos de gran propagación, la vacuna suele estar disponible entre 12 y 24 horas después de las primeras infecciones, tiempo más que suficiente para que el virus logre autoenviarse a miles de sistemas aprovechando Internet. El problema se agrava si tenemos en cuenta los desfases que ocurren entre la aparición de la vacuna y la actualización por parte de los usuarios. A continuación los resultados obtenidos en la Encuesta AntiVirus 2001 - Hispasec, llevada a cabo hace unas semanas sobre más de 2000 usuarios que participaron en el test EICAR.

Cada cuanto tiempo suele actualizar su antivirus:

Todos los días -> 23,46%
Dos o tres veces por semana -> 15,64%
Una vez a la semana -> 29,62%
Dos o tres veces al mes -> 14,10%
Una vez al mes -> 11,28%
Trimestralmente -> 2,82%
No suele actualizarlo -> 3,08%

Tuvimos ocasión de comentar este problema con Eugene Kaspersky y Mikel Urizarbarrena, presidentes de AVP y Panda Software respectivamente, con motivo de la Comparativa Antivirus 2001 de Hispasec (http://www.hispasec.com/comp_avs2001.asp?id=18). Ambos coincidieron en apuntar a la heurística como solución, si bien queda patente que sigue resultando trivial crear virus que burlen este tipo de detecciones genéricas.

Otras soluciones más genéricas pasan por el uso de la criptografía. En la misma comparativa antivirus abordamos esta posibilidad en el caso concreto de Windows XP y el uso de la firma digital a nivel de aplicaciones (http://www.hispasec.com/comp_avs2001.asp?id=28).

Visto que aún existe un gran número de usuarios que hacen oídos sordos a la regla de oro de no abrir archivos adjuntos no solicitados, que los antivirus no planean modificar su esquema actual y que tampoco esperamos que Microsoft resuelva este problema a nivel de sistema operativo, vamos a proponer una solución intermedia.

Actualizaciones Urgentes Automatizadas

Como hemos visto, el desfase de tiempo entre la aparición en escena del virus y la protección efectiva del usuario es debido en su mayor parte al proceso de actualización del antivirus. La mayoría de las soluciones dejan esta acción a discreción del usuario, que debe activarla manualmente.

Existen otras soluciones que permiten automatizar estas descargas, si bien los tiempos no suelen ser inferiores a 24 horas y aún son muchos los usuarios reticentes a que el antivirus decida cuándo descargar cientos de kilobytes sin tener en cuenta que puede consumir ancho de banda en detrimento de otros servicios que se estén utilizando en ese momento, como descarga de otros archivos, juegos en línea, vídeoconferencias, etc.

La propuesta consiste en que el antivirus pueda detectar la necesidad de una actualización urgente, cómo por ejemplo la de SirCam, y proceder a la descarga automatizada de su correspondiente vacuna. La comprobación periódica a través de Internet mientras el usuario está conectado no tiene por qué consumir más que unos pocos bytes (puede ser inferior a 1 Kb a la hora), tráfico insignificante que no supone molestia alguna para el usuario.

Ante la detección de una alerta, la casa antivirus sólo tendría que modificar el estado en su servidor y los antivirus procederían a la descarga automática de la vacuna de forma casi inmediata. El tráfico producido en el caso de alerta también sería mínimo, pues incluiría la vacuna específica para el virus en lugar de las actualizaciones diarias o periódicas que suelen incluir información sobre decenas de especímenes.

Bernardo Quintero

14/11/2001 Legislación norteamericana contra los análisis de seguridad

Recientemente, EE.UU. ha aprobado una serie de leyes encaminadas a declarar ilegales la publicación de estudios y análisis que demuestren vulnerabilidades en sistemas hardware o software. Las leyes, englobadas bajo el nombre común de DMCA (Digital Millennium Copyright Act), pretender defender las industrias de contenidos (audio, texto y vídeo) frente a la piratería, pero sus implicaciones son muy amplias y peligrosas.

La DMCA convierte en ilegal la distribución de “circumvention technology” (tecnología para burlar protecciones). Entendido en un sentido amplio, algo que ya se está aplicando en EE.UU., un documento científico describiendo una vulnerabilidad en una tecnología entraría dentro de esta categoría y, por lo tanto, sería ilegal en los Estados Unidos.

Publicar casi cualquier trabajo sobre seguridad, entonces, sería un acto delictivo en ese país.

A este respecto me gustaría exponer una serie de conclusiones, a título personal:

* Aunque publicar información sobre vulnerabilidades sea ilegal, la información seguirá circulando libremente por el mundo "underground", donde el anonimato es ley. En cambio, los administradores de sistemas y responsables de seguridad, siendo personas legales, no tendrán acceso a esa información, que sí tendrán sus atacantes.

* El progreso técnico y científico se basa en el libre flujo de información y en estudios independientes. Esto es especialmente cierto en el campo de la criptología. Si los problemas de diseño o implementación de un sistema criptográfico no se pudiesen hacer públicos de forma legal, los usuarios tendrán sistemas débiles e inseguros.

Ya existen casos demostrables en los que una tecnología criptográfica, una vez expuesta a expertos independientes, se ha demostrado insegura: el cifrado GSM, la protección anticopia de los DVDs, el cifrado WEP de las redes inalámbricas 802.11... Si dichas tecnologías se hubiesen hecho públicas, el descubrimiento de sus vulnerabilidades se habría efectuado antes de llegar al mercado.

¿Qué hubiera ocurrido si la publicación de las vulnerabilidades fuese ilegal?. La vulnerabilidad seguiría existiendo, por supuesto, y sería conocida dentro de determinados círculos. El público, no obstante, pensaría que está utilizando tecnología segura y de calidad, estando a merced de tiburones sin escrúpulos.

Adicionalmente, sin la publicidad de las vulnerabilidades, las empresas no tendrían ningún aliciente para seguir innovando y dotar a los sistemas, aunque sea tras infinidad de intentos fallidos, de verdadera seguridad a toda prueba.

Los primeros resultados negativos ya se han empezado a ver:

* La versión 2.2.20 del kernel Linux, de reciente aparición, indica expresamente en su fichero de "cambios" que se han solucionado varios problemas de seguridad, pero que no se proporcionan detalles para no violar la DMCA.

* Un ciudadano ruso, de nombre Dmitri Sklyarov, está pendiente de juicio en EE.UU., al ser coautor de un programa utilizado para descifrar ficheros PDF. El programa, elaborado y distribuido por una firma rusa, se vende desde ese país. Dimitri está acusado de contravenir la DMCA, aunque sea ciudadano extranjero y los actos de los que se le acusa se realizasen fuera de los EE.UU.. Dimitri fue detenido por el FBI, tras una denuncia de Adobe, al término de una jornadas de seguridad desarrolladas en los Estados Unidos, a donde había viajado desde su país natal. El trabajo de Sklyarov es perfectamente legal en Rusia y en la mayoría de los países occidentales.

Si tienes más de un hijo, ¿puedes ir de vacaciones a China sin peligro de ser encarcelado, al haber violado una ley local de ese país, mientras estabas en el exterior y siendo ciudadano foráneo?. Probablemente en China sí, pero no en los Estados Unidos, si se ven los precedentes.

* El profesor Edward Felten, de la universidad de Princeton, decidió no publicar los fallos de seguridad que había descubierto en el reto SDMI (Secure Digital Music Initiative), con los que probaba que era posible eliminar las "marcas de agua" insertadas en una canción, destruyendo el sistema anticopia puesto a prueba por la SDMI. A pesar de que el objetivo del reto era demostrar si los sistemas propuestos eran

seguros, algo que Felten echó por tierra, publicar sus resultados sería ilegal. En ese sentido, la industria discográfica seguía intentando aprobar un esquema de protección musical demostradamente fallido, aunque las pruebas de ello no fuesen públicas, y el autor de las mismas tuviese que afrontar denuncias judiciales.

* Recientemente Niels Ferguson, criptógrafo holandés de reconocido prestigio internacional, afirmó haber descubierto una vulnerabilidad en el esquema de protección HDCP de Intel. HDCP es un sistema de cifrado para el bus DVI, donde se conectan televisores, cámaras, reproductores de DVD y similares. Según Ferguson, se puede obtener la clave maestra del sistema en menos de dos semanas. Una vez obtenida dicha clave, se pueden copiar o crear contenidos sin restricción, crear dispositivos nuevos, etc.

Aunque Ferguson no publicó los detalles (aunque es holandés, podría ser detenido en cualquiera de sus viajes a EE.UU.), poco después se desvelaron todas las interioridades de forma abierta, a través de otra vía: Scott A. Crosby, de la universidad Carnegie Mellon. Estudiándolas detenidamente, se puede observar que la seguridad del sistema HDCP es trivial.

Como se cita a Ferguson en el semanario Ciberpaís: “Si no investigamos, nunca desarrollaremos buenos esquemas de protección anticopia. La DMCA protege al fabricante de un mal producto en el sentido de que es ilegal demostrar que es defectuoso”. De hecho la DMCA contraviene sus propios intereses, ya que sin poder investigar sistemas anticopia avanzados es imposible desarrollar esquemas seguros.

El problema de la DMCA no son tanto sus objetivos sino los medios que aborda para ello. La discusión de vulnerabilidades o la posesión de sistemas capaces de saltarse protecciones no debe ser algo ilegal, sencillamente porque existen multitud de usos legales para esa tecnología e información.

Los cerrajeros, por ejemplo, necesitan disponer de sus herramientas de forma legal. Las empresas de recuperación de datos necesitan herramientas de escaneo de discos duros a bajo nivel para poder hacer su trabajo.

Las herramientas y los conocimientos no deberían ser ilegales si tienen usos beneficiosos. Lo que debe ser ilegal, y ya lo es en la mayor parte de los países, es la copia, venta y distribución no autorizada de material protegido con “copyright”. Esa legislación ya existe y se utiliza constantemente desde hace decenios. La DMCA, en su estado actual, no tiene ningún sentido.

Prohibir difundir un documento porque su temática no nos es grata es algo prohibido (salvo casos excepcionales) en la mayor parte del mundo “civilizado”, tratándose de un derecho garantizado con leyes que promueven la libertad de expresión y la libertad de prensa. Es triste comprobar como el país del mundo que se vanagloria de mayor libertad tira por tierra su “Primera Enmienda” constitucional con una ley que ni siquiera cumple sus objetivos declarados. El reciente fallo judicial catalogando el código “DeCSS” como protegido por la libertad de expresión, hecho del que nos hicimos eco en Hispasec esta misma semana, abre una brecha legal para atacar la DMCA. Cuando el juicio de Dmitri Sklyarov empiece (Dmitri está actualmente en libertad provisional y tiene prohibido abandonar EE.UU., aunque es ruso y reside en Rusia) no sería sorprendente que la DMCA fuese declarada anticonstitucional.

Mientras tanto, seguiré teniendo mucho cuidado con lo que digo, aunque sea español y no tenga pensado viajar a EE.UU. en un futuro próximo...

Recomiendo a todos los lectores de “Una-Al-Día” que echen un detenido vistazo a los enlaces que siguen.

Jesús Cea Avión

Entrevista



Jorge Ramió Aguirre

Hablar de **Jorge Ramió** es hablar de criptografía y seguridad en España y Latinoamérica. Es Ingeniero de Ejecución en Electrónica por la Universidad del Norte de Arica en Chile, Dr. Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y actualmente cursa el Máster y Doctorado en Ingeniería de Sistemas y Servicios Accesibles para la Sociedad de la Información en la UPM. Entre otras asignaturas, en la Escuela Universitaria de Informática EUI ha sido profesor desde el curso 1994/1995 de la asignatura Seguridad Informática. Desde el curso 2004/2005 es coordinador de la asignatura Gestión, Auditoría, Normativas y Legislación en Seguridad Informática que en el curso 2007/2008 pasa a llamarse Temas Avanzados en Seguridad y Sociedad de la Información. Desde 2006 imparte junto a la profesora Ángeles Mahíllo la asignatura Historia de los Códigos Secretos en formato e-learning. Además es creador y Coordinador de la Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed desde diciembre de 1999 y Director de la Cátedra UPM Applus+ desde mayo de 2006. Alienta y motiva a sus alumnos como nadie. Le gusta lo que hace y eso se nota.

Hispasec: ¿Cuál y cómo fue tu primer contacto con Hispasec?

Jorge Ramió Aguirre: En el mes de diciembre de 1999 creé la Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed, justo un año después del nacimiento de Hispasec; es decir, somos casi de la misma quinta. Las razones de su creación no son el caso comentarlas aquí, pero seguramente coincidirían con algunas de las razones por la que Hispasec hizo su aparición en la Red: el auge ya comprobado en esos años de la seguridad informática, una especie de efervescencia académica y ganas de hacer cosas en este área por parte de las universidades y la convicción certera de que esto de la seguridad seguiría creciendo, como así ha sido.

Recuerdo que una de las primeras cosas que hice al crear la red fue ponerme en contacto con Bernardo Quintero y presentarle el proyecto. De hecho, en una-al-día del 23 de abril del año 2000 aparece dicha presentación y contesto a algunas cuestiones que Bernardo me plantea con respecto al proyecto. En esa fecha la red temática contaba con 110 miembros; hoy en día, nueve años después, los miembros son más de 730, ambos nos hemos hecho mayores de edad.

H: ¿Estás suscrito a una-al-día? ¿Desde cuándo?

JRA: De acuerdo a lo comentado en la pregunta anterior, mi fecha de alta en una-al-día debería estar en torno al primer trimestre del año 2000. Más de ocho años recibiendo ese servicio, casi desde sus inicios, no está mal.

H: ¿Cómo influyó una-al-día e Hispasec en la difusión de CriptoRed?

JRA: Sin lugar a dudas muy positivamente. Primero que nada, debo decir que dicho servicio es muy bien valorado en toda Latinoamérica, países a los cuales se difunde preferentemente la información que se genera en la red temática, y que su Resumen de Actualidad número 5 correspondiente al mes de febrero de 2001 ya se publica en una-al-día, y así ininterrumpidamente durante más de 80 meses.

Últimamente la media de accesos a CriptoRed se sitúa sobre los 1.200 diarios. Cuando en Hispasec se publica en una-al-día dicho resumen, esos accesos se sitúan sobre los 2.000 el primer día de su publicación y en torno a los 1.500 el segundo día. Por tanto, se puede concluir que hay muchos usuarios de este servicio de Hispasec que esperan mes a mes tales resúmenes de la red temática, preferentemente para descargarse

los nuevos documentos que habitualmente se suben a dicha red. En conclusión, debo estar muy agradecido de Hispasec por hacer llegar a decenas de miles de usuarios los contenidos de CriptoRed.

H: ¿Cuál es el sitio más interesante en el que has estado por trabajo?

JRA: Podría decir que mi visita a vuestras dependencias en Málaga, pero sonaría a peloteo. Creo que no hay un sitio en especial y no es que mi vida profesional sea aburrida ni mucho menos; por ejemplo no he tenido aún ocasión de visitar Bletchley Park ni otros museos similares. Por la red temática que coordino, he visitado desde el año 2000 la práctica totalidad de los países latinoamericanos por razones de promoción de dicha red o bien invitación a congresos y cursos, algunos de ellos en varias ocasiones, y de todos me he traído excelentes recuerdos. Ahora bien, si en vez de sitios modificamos la pregunta por personas, en este caso diría que conocer y compartir conversación y experiencias con Martin Hellman y Alfred Menezes, dos pesos pesados de la criptografía mundial y que he tenido la suerte de invitar a congresos DISI y CIBSI que he organizado: como casi siempre sucede en estos casos, te das cuenta que son excelentes personas y de una humildad increíble con todo lo importantes que son.

H: ¿Piensas que se ha perdido el "romanticismo" de aquellos primeros días en la red?

JRA: En general, es muy posible que sí. Ambientando esta pregunta en el entorno hacker, está claro que la respuesta es afirmativa. Hoy prima el negocio, se están acabando los hackers que tenían bien ganado ese apellido de ser la conciencia de la red, se desea ganar dinero lo más rápidamente posible a costa de lo que sea y sin contar para nada con unos mínimos principios éticos. Estamos avanzando a pasos agigantados en el cibercrimen y los problemas que esto traerá no sólo a las personas sino a los países no serán muy agradables. Cierto es que siempre habrá quienes estén preocupados de que los sistemas sean más seguros (sin ir más lejos Hispasec entre ellos) pero al igual que sucede con las leyes, los malos irán por delante y los buenos persiguiéndoles y poniendo parches. Pero volviendo al sentido de tu pregunta, también es cierto que los primeros años de Internet y del correo electrónico, finales de los 80, fueron maravillosos porque todo era novedad, éramos como chavales ante una nueva consola con prestaciones insospechables.

H: ¿Cómo y por qué te metiste en esto?

JRA: Pues muy sencillo. Corría el año 1990 y en la Escuela Universitaria de Informática de la UPM donde trabajo, en el departamento de LPSI, se preparaba el nuevo Plan de Estudios para 1992. Los profesores que así querían podían proponer nuevas asignaturas optativas y estuve dudando entre proponer una asignatura relacionada con la ofimática o bien una de seguridad informática. En ambos temas se comenzaba desde cero pero había suficiente tiempo para su preparación porque las primeras clases serían en el curso 1994/1995. No sé muy bien por qué me decidí por la de seguridad, pues la ofimática estaba muy de moda en esos años; tal vez por ser un desafío más interesante y tener un campo más amplio. No me equivoqué y no me arrepiento; en estos 15 años he visto cómo se ha desarrollado la oferta académica de estas asignaturas: de las más de 100 asignaturas similares que se ofrecen en las universidades españolas en la actualidad, la de Seguridad Informática que imparto desde 1994 se encuentra entre las 10 más antiguas. Un dato importante: cuando comencé en esto seguramente seríamos en España unos 50 a 75 profesores dedicados a la seguridad y en la actualidad estamos en torno a los 400. Teniendo en cuenta la baja contratación de nuevo profesorado en las universidades desde más de una década a esta parte, este espectacular incremento en la oferta y grupos de seguridad habla por sí solo de la importancia de la misma.

H: ¿Cuáles eran los principales retos a finales de los noventa?

JRA: Aunque sea simplificar mucho las cosas, en los comienzos de los años noventa se repetía hasta el

cansancio lo de confidencialidad, integridad y disponibilidad, y digamos que poco más. A finales de esa década, ya con el desarrollo masivo de Internet, recuerdo haber pasado de claves RSA de 512 a 1.024 bits, y de los 40 bits de clave simétrica en una sesión SSL a los 128 actuales, de un día para otro, algo impresionante. El reto por excelencia era encontrar un nuevo algoritmo de cifra simétrica estándar, dado que el DES había ya sucumbido a un ataque en red y sin embargo seguía siendo el estándar de cifrado simétrico. A finales de la década llegó el concurso del AES y ya todos sabemos la historia.

No obstante, humildemente siempre me pregunto cómo es que se ha pasado tan rápidamente de una paranoia total en cuanto a la limitación de la longitud de las claves en función de los países, las restricciones para las exportaciones de productos criptográficos, etc., a la democratización (por hacer un símil) total de la criptografía. Hoy en día encuentras en Internet implementaciones del código fuente del AES en decenas de lenguajes.... con el cibercrimen en aumento e incluso manifestaciones claras de guerra digital e information warfare, aquí nadie se rasga las vestiduras. Tal vez haya gato encerrado. Quien haya leído el libro Cripto de Steven Levy, deberá concluir que obviamente algo ha cambiado en nuestros días, al menos en la famosa triple alambrada.

H: ¿Para cuándo una carrera universitaria específica de Seguridad TIC?

JRA: Buena pregunta. De momento no la hay, al menos en España. Pero los tiempos cambian y mira por dónde en los nuevos planes de estudio de mi escuela orientados hacia la convergencia con Bolonia, se impartirán las nuevas titulaciones de Graduado en Ingeniería del Software y Graduado en Ingeniería de Computadores, y en ambas aparecen "Fundamentos de la Seguridad de la Información" y "Seguridad en Redes" como asignaturas obligatorias y con una amplia carga lectiva. Algo por lo que muchos profesores veníamos años suplicando, al menos en mi caso desde el año 2.000 en que tuve la osadía de proponer en un congreso celebrado en Palma de Mallorca una nueva titulación específica en seguridad informática. Esto puede ser una quimera, pero opino que tal vez no vendría mal al menos analizar esa posibilidad y hacer un estudio de mercado. Lo que sí es cierto es que en España abundan ofertas de postgrado en seguridad desde distintas universidades y organismos, superando en la actualidad las 15, un número muy a tener en cuenta si lo comparamos con otras especialidades de la informática y las telecomunicaciones más antiguas y, supuestamente, con más cuota de mercado. Si a eso unimos el momento incierto por el que pasa el mercado tradicional de la informática en nuestro país, tal vez nos llevaríamos más de una sorpresa.

Pensado sólo en la faceta civil, puesto que la militar va por otros derroteros más estrictos, la seguridad no sólo está de moda sino que es necesario contar con ella en todos los niveles de diseño, producción, gestión y auditoría. Además, desde hace poco más de un lustro muchos de sus procesos son de estricto cumplimiento de acuerdo con las actuales leyes de protección de datos y normas internacionales, con lo cual se cierra el ciclo en tanto tales procesos deben ser auditados. Sinceramente, no se puede pedir más. Tienes razón, hace falta una nueva titulación en Seguridad TIC; el tema está en quién está dispuesto a llevarse el gato al agua y comenzar casi desde cero con esta oferta; no es fácil y mucho menos en el momento que vive actualmente la universidad española.

H: ¿Por dónde andarán los tiros en seguridad en el futuro?

JRA: Sinceramente creo que esto no hay quién lo conteste; como dijo Niels Bohr "predecir es muy difícil, especialmente el futuro". No obstante, se supone que el advenimiento de la computación cuántica con equipos estables y a un coste razonable significará un cambio radical en los actuales conceptos criptográficos. Mucha gente opina que esto nunca llegará a ser una realidad por el tamaño actual de estos equipos y sus altos costes; pero debemos recordar que lo mismo se decía hace 40 años sobre aquellos computadores a válvulas de vacío y de tamaños descomunales y todos sabemos a lo que hemos llegado en

cuanto a miniaturización.

Para lo que no hace falta ser un adivino es para indicar que la seguridad de la información irá cada vez teniendo una mayor importancia en nuestra sociedad, en instituciones y empresas y que, por lo tanto, sigue siendo una excelente salida profesional para nuestros futuros ingenieros.

H: ¿A qué dedicas más tiempo últimamente?

JRA: A leer una-al-día... bueno, digamos que algo más. Bromas aparte, además de impartir tres asignaturas relacionadas con la seguridad informática en mi universidad, participo como profesor invitado en 5 postgrados en Latinoamérica, soy director de la cátedra UPM Applus+ que organiza todos los años el Día Internacional de la Seguridad de la Información DISI, congreso gratuito que este año trae a Madrid a la Dra. Radia Perlman de Sun Microsystems (quien no conozca a "la Madre de Internet" que busque en Google) el 1 de diciembre de 2008, y coordino CriptoRed que entre otras cosas organiza en América Latina un Congreso Iberoamericano de Seguridad Informática todos los años impares, de forma que la quinta edición de CIBSI se celebrará en noviembre de 2009 en Montevideo, Uruguay, nada menos que en la famosa torre Antel de dicha ciudad (lo mismo, quien no la conozca que busque en Google). Hay otras actividades paralelas como colaboración en proyectos de investigación y desarrollo, informes técnicos, etc., pero creo que sólo con esto es ya suficiente como para decir que no tengo demasiado tiempo libre, lo cual como todos sabemos no es nada saludable.



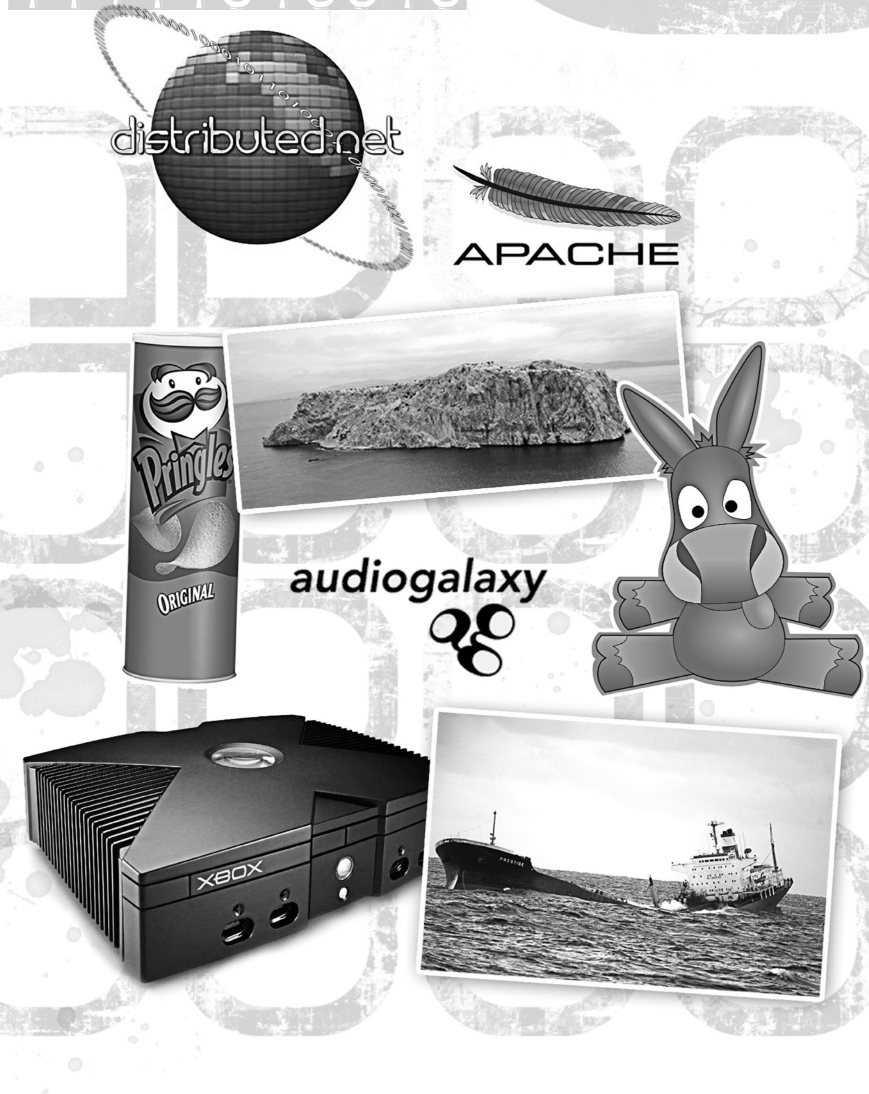
7D2

3722

Capítulo 4

AÑO 2002

11111010010



1009843200 – 1041379199



Durante este año...

_ **“¿En euros o en pesetas?”** El 1 de enero comienzan a circular en doce estados, las monedas y billetes físicos de euro. Se populariza como regalo una bolsa de 12 euros con las diferentes monedas, que puede adquirirse en bancos. La peseta y el euro convivirán durante tres meses, y en todas las tiendas se repite la misma pregunta “¿Vas a pagar en euros o en pesetas?”. A las pocas semanas se descubre que ciertas sustancias en las monedas provocan alergias en la población. El 1 de marzo desaparece la peseta como moneda de curso legal, pero todavía podrá cambiarse en el Banco de España.

_ Se prohíbe por ley la venta de cualquier tipo de **gasolina con plomo**.

_ La película **“Los otros”**, de Alejandro Amenábar, se convierte en triunfadora de los Premios Goya con ocho galardones.

Mircrosoft entra de lleno en el mercado de las consolas de videojuegos con la **Xbox**. Es la primera consola en incorporar un disco duro, pensado para almacenar partidas guardadas. Su precio es de unos 300 dólares. Cuenta con una CPU de 733 Mhz y una RAM de 64 megas. A principios de 2002 ya había sido lanzada en Estados Unidos. Su integridad dura poco más de un mes. Un estudiante del Instituto de Tecnología de Massachusetts publica el código de su BIOS. Informa con todo lujo de detalles de todo el proceso en su página web, junto con documentación variada sobre su funcionamiento. El estudiante recibe una llamada telefónica de un alto cargo de Microsoft y cuelga en su web el mensaje que deja en su contestador. Todavía está disponible en la dirección http://web.mit.edu/bunnie/www/proj/anatak/xboxedited.mp3. Más tarde, en junio de ese mismo año, se publicarían los detalles técnicos de todo el proceso de arranque, y se describiría una vulnerabilidad que permite instalar software en la máquina. Todo fue posible gracias a tres semanas de trabajo de un ingeniero inverso y 50 dólares en material.



_ En febrero, la sonda espacial **Mars Odyssey** comienza a cartografiar la superficie de Marte a través de un sistema térmico. En mayo se encuentran signos de depósitos de hielo en el planeta.

_ Las autoridades británicas autorizan el nacimiento de **un bebé probeta, genéticamente seleccionado**, para intentar salvar la vida de su hermano enfermo.

_ El 23 de febrero **Íngrid Betancourt**, candidata a la presidencia, y su jefa de debate Clara Rojasson son secuestradas por las FARC en Colombia. Serían liberadas más de seis años después.

_ El dinero está barato en Estados Unidos. Las **hipotecas** se conceden a cualquiera, sin avales, sin garantías. Incluso con solo responder a un correo basura, donde se comienzan a anunciar bancos

fantasmas de forma masiva, regalando **“mortgages”**. Se establece el germen de la crisis económica de 2008 (calificada como la peor desde 1927).

_ En el **campeonato del mundo de fútbol** de 2002, España vuelve a caer en cuartos ante Corea del Sur.

_ El 20 de junio los sindicatos UGT y CC.OO convocan la **segunda huelga general en España**. Su seguimiento sería importante, pero menor que la que tuvo lugar el 14 de diciembre de 1988, en la que ocasionó gran impacto el hecho de que toda RTVE dejase de emitir al unísono. Ambas huelgas estaban destinadas a protestar contra reformas laborales introducidas por el gobierno.



_ El 11 de julio un grupo de gendarmes marroquíes toma la **Isla Perejil**. Se trata de un islote deshabitado a 8 kilómetros de Ceuta reclamado alternativamente tanto por España como por Marruecos, que se encuentra en un limbo legal sobre a quién pertenece realmente. Marruecos exige su soberanía sin dudas jurídicas sobre el islote y reivindica que forma parte de su territorio nacional. En verano de 2002 desafía a España, tras una escala de incidentes diplomáticos en los que se crearon tensiones entre ambos países, seis gendarmes toman la isla por sorpresa. Poco después son sustituidos por soldados. El gesto de Marruecos es tachado de inamistoso por la OTAN y España entra en el primer incidente armado tras la democracia, en una simple operación militar que duraría apenas unas horas, pero en la que se despliega un pequeño y desproporcionado ejército. El 20 de julio España recogería su bandera y el islote volvería a quedar deshabitado.

_ En septiembre, **George W. Bush** desafía a los miembros de Naciones Unidas, para que afronten el “grave y creciente peligro” que representa Iraq o, de lo contrario, se mantengan al margen de los actos que los Estados Unidos y aliados pudieran realizar.

_ Comienza el proyecto **emule**. Después del cierre de Napster, aparecen alternativas como WinMX (que cerraría en 2005) e iMesh, pero ninguno destaca por encima del resto. Llega Audiogalaxy y con él la época dorada del intercambio de archivos musicales. Mucho más completo y eficiente que Napster, también desaparecería por presiones de la RIAA. Se utiliza mucho eDonkey2000, pero el programa cada vez contiene más spyware y es poco eficiente... entonces llega emule, programa abierto y gratuito que se impone con fuerza desde ese momento y hasta nuestros días. La compañía propietaria de eDonkey2000, MetaMachine, también alcanzaría un acuerdo en 2006 con la RIAA para evitar un juicio por violar de los derechos de propiedad intelectual. Tuvo que pagar una compensación de 30 millones de dólares.

El 19 de noviembre se parte en dos, con 77.000 toneladas de fuel dentro, el petrolero **Prestige** en las costas de Galicia, a 250 kilómetros de Finisterre. Antes de hundirse definitivamente, cuando se detecta el daño en el casco del barco y la potencial catástrofe, el gobierno, las empresas de salvamento y el capitán del barco comienzan unas fracasadas negociaciones con las que no llegan a ningún acuerdo. La situación es crítica y cada minuto cuenta. Mientras, se especula sobre si es mejor alejarlo o acercarlo a las costas gallegas: el valor de la mercancía que lleva alcanza los 60 millones de euros, y no se quiere correr el riesgo ni de arruinar las costas de ningún país, ni de perder por completo el cargamento.



Finalmente el petrolero es remolcado lejos de las costas gallegas, se intenta evitar la contaminación de las Rías Bajas. El presidente de la Junta de Galicia, Manuel Fraga, asegura que el hundimiento no tendría efectos sobre el medio ambiente. Más tarde Aznar reconoce errores de apreciación. Cuando la nave se hunde, se derramaron 63.000 toneladas de fuel-oil al océano. Comienza a llegar a la costa el chapapote en forma de galletas compactas de fuel que destroza las playas, la flora, los peces y las aves. Durante todo 2003, se produciría una avalancha espontanea de voluntarios que acuden a limpiar altruistamente las playas equipados con monos blancos. Se recogen a mano los restos de crudo derramado que se escapa del barco hundido. El 10 de septiembre de 2004 Repsol-YPF daría por finalizada la tarea de extracción del fuel del barco hundido.

Seguridad Informática



_ A principios de año se detecta SWF.LFM.926 un virus muy primitivo capaz de infectar los archivos de Shockwave Flash (extensión .swf). Se trata de una prueba de concepto, sin riesgo real, que demuestra la posibilidad de realizar un comportamiento vírico en formatos no habituales.

_ Aparece un virus como prueba de concepto capaz de infectar a la plataforma .NET.

_ El usuario no aprende, y los internautas que se conectan por primera vez a Internet se dejan engañar de nuevo. A principios de 2002 rebrota con fuerza el bulo del archivo de Windows **Sulfnbk.exe**.

_ En enero se presenta la especificación **SAML** para su revisión pública, un fallido intento de crear un estándar para el intercambio de información de autorización y autenticación. Security Assertion Markup Language (SAML, que se pronuncia "samul") es un entorno basado en XML especialmente diseñado para facilitar el intercambio de información de autenticación y autorización entre los diferentes componentes de la infraestructura de seguridad informática.

_ Virus como **Myparty**, aunque sin ninguna aportación técnica al género, triunfan por ingeniería social. El asunto del correo con el que se distribuye es "new photos from my party".

Bajo el nombre de **Strategic Technology Protection Program** (STPP) Microsoft presenta una iniciativa que pretende mejorar la seguridad de sus sistemas operativos y su respuesta ante nuevos problemas de seguridad. El programa Strategic Technology Protection Program (STPP) es una iniciativa por la que Microsoft pretende proporcionar herramientas gratuitas y soporte técnico a empresas de cualquier tamaño. Propone entre otras medidas un teléfono de asistencia gratuita para ayudar a los clientes a resolver incidencias originadas por un virus, asesoramiento acerca del modo de instalar actualizaciones de seguridad... Microsoft también se compromete a publicar de forma sistemática y bimensual (aunque esta periodicidad nacería ya como los famosos parches mensuales) los conjuntos de actualizaciones de seguridad. Se establece la idea de un sistema central de gestión de

actualizaciones (lo que mas tarde se convertiría en los exitosos Software Update Services, Windows Software Update Services, Microsoft Operations Manager...).

Microsoft se toma en serio su "Trustworthy Computing" o "Informática de Confianza" que anunció tras llegar a lo que (por aquél entonces) se creía techo de la inseguridad y problemas acarreados por el sistema operativo Windows y sus productos. Poco después, cuando todavía comenzaba a dar los primeros pasos hacia la implementación real de este nuevo concepto de introducción de seguridad en sus productos, virus como Blaster fueron mucho más allá y la situación se volvería casi insostenible.

_ Hewlett-Packard publica una distribución comercial Linux con novedosas características de seguridad, llamada Linux **HP-LX 1.0.** Está basada en RedHat 7.1.

_ Se decubren nuevos ataques contra la privacidad. Microsoft recopila información de la música y vídeos reproducidos a través de **Windows Media Player 8** sin avisar. La información recopilada, aunque limitada, puede formar junto con otras un perfil del usuario. Una vez procesada la información, Microsoft devuelve y almacena en el sistema del usuario un archivo en el que se reflejan las preferencias del usuario.

_ En marzo, la **vulnerabilidad de los routers ADSL de Telefónica** que se descubriera dos meses atrás, se comienza a aprovechar de forma masiva por atacantes. Los routers son los Efficient SpeedStream 5660. Se cometió un error que provocaba que los filtros IP no funcionasen. Los filtros IP se utilizan, por ejemplo, para limitar el acceso administrativo del router a ciertas IPs. Si los filtros no funcionan, cualquier atacante que conozca la clave puede acceder a ellos y realizar los cambios que desee. Como las claves de los ADSL de Telefónica son todas iguales y, en la práctica, la contraseña en cuestión es de dominio público (adminttd, adminttd), a efectos prácticos cualquier usuario de Internet puede conectarse a esos router y manipularlos de forma arbitraria.



_ Se populariza el gusano **W32.Gibe.dam** que simula ser una actualización de seguridad que Microsoft envía por correo.

_ En marzo sale a la luz uno de los hacks más famosos de la historia. **El acceso a Internet gracias a los tubos de galletas Pringles**. Las redes inalámbricas empiezan a despuntar en todo el mundo y surgen proyectos para compartir la conexión entre usuarios de la mismas ciudades. La BBC informa de que los tubos vacíos de galletas Pringles pueden convertirse en unos útiles (y baratos) amplificadores de las señales de radio. Gracias a la particular forma del tubo de Pringles, es posible usarlo como amplificador y antena direccional.

_ **Klez.H**, variante del original virus Klez, es oficialmente proclamado el mayor virus de toda la historia, robando el puesto a SirCam, Melissa e incluso al famoso I Love You, uno de los más populares. Se registran 20.000 copias del virus cada día, con una media de una infección por cada 300 correos electrónicos que circulan por Internet. Disfraza los correos infectados con asuntos completamente aleatorios. Las sucesivas modificaciones del código del Klez original dan lugar a nuevas variantes mucho más complicadas de detectar y cada una de ellas más popular que la anterior entre la comunidad afectada.

_ En mayo, un matemático japonés c**onsigue engañar a once lectores de huellas digitales** invirtiendo menos de 10 dólares en material y una hora de trabajo. Tsutomu Matsumoto duplicó una huella digital resaltando su impresión sobre cristal (por ejemplo, un vaso o una ventana) mediante adhesivo de

cianoacrilato (comercialmente distribuido con marcas tan conocidas como “Super Glue”) y fotografiando el resultado con una cámara digital. La imagen resultante se mejoró mediante Photoshop y se imprimió en una hoja de papel transparente. Matsumoto utilizó la hoja como máscara para generar un circuito impreso con la imagen de la huella digital (para proporcionar “relieve”). Seguidamente obtuvo un dedo de “gelatina” empleando el circuito impreso para proporcionarle el relieve que emula la huella digital original. El resultado: un “dedo” que pasa la prueba de un escáner digital con una efectividad del 80%. Se cree que la biometría es el futuro de la informática. Incidentes como este harían que, muchos años después, siga sin llegar con éxito rotundo a la informática de consumo.

_ Las tres ramas de **BIND** sufren constantes problemas de seguridad durante todo el año. Todavía se mantienen activas la 4, la 8 y la 9.

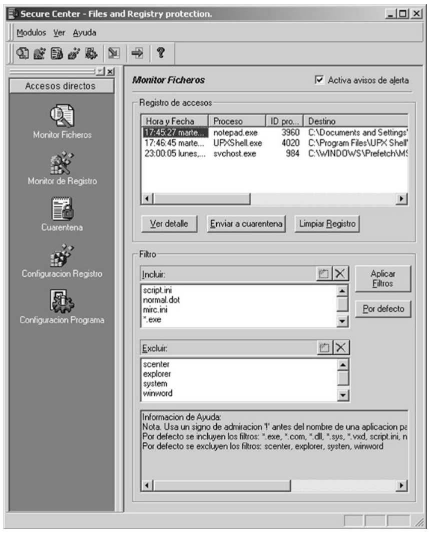
_ **Apache** es el servidor web más popular del mundo, con más del 60% de cuota de mercado. Se descubre que las versiones de Apache previas a la 1.3.26 y 2.0.39 son susceptibles a un ataque realizado a través de cabeceras incorrectas en los “chunked data”. Los “chunked data” (datos troceados) permiten enviar segmentos de datos de forma paulatina, por ejemplo, si no se conoce el tamaño final de los datos pero se quiere realizar la transmisión a medida que se van obteniendo, en vez de esperar a tenerlos todos. Se trata de una modalidad de protocolo HTTP poco utilizada. Las versiones de Apache vulnerables no gestionan adecuadamente la presencia de valores ilegales en la cabeceras “chunked data” y esto puede permitir la ejecución de código. No tardan en aparecer exploits y se convierte en una grave vulnerabilidad.

_ La Agencia Federal de comunicación e Información del gobierno ruso declara a bombo y platillo que el nuevo sitio web del presidente www.president.kremlin.ru está blindado contra ataques. Recuerda a la sonada campaña de Oracle cuando presentó su versión 9i con el nombre de **“Unbreakable”**, (irrompible). A finales de 2001 Internet se llenó de anuncios y banners que prometían que la nueva versión de Oracle era irrompible. Entre la comunidad, este mensaje perteneciente a una agresiva campaña de marketing no pudo más que tomarse a broma. No tardaron en aparecer todo tipo de desbordamiento de memorias intermedias, fallos remotos, locales, internos, exploits... algunos incluso obvios y triviales. El software de Oracle seguía siendo vulnerable a todo tipo de fallos de seguridad, tanto o más que sus predecesores y, con el tiempo se sabría, menos que sus sucesores. La campaña todavía se recuerda por lo pretenciosa y popular que resultó. Nunca más Oracle usaría esa campaña.

_ En junio de 2002 se encuentra un grave **fallo de seguridad en OpenSSH** que permite a un atacante remoto obtener total control del sistema.

_ Ross Anderson publica un estudio analizando la iniciativa de Intel, HP, IBM y Microsoft denominada **“Trusted Computing Platform Alliance”** (TCPA, que en 2003 se convertiría en la Trusted Computing Group). Se supone que su objetivo es que la nueva generación de ordenadores personales sean más seguros, pero según Anderson, el objetivo real es aumentar la seguridad en aquello que interesa a los fabricantes de ordenadores y de software, en contra de los intereses reales de los usuarios de los mismos en materia de seguridad. Además Anderson afirma que la TCPA , si prospera, puede ser una amenaza directa a la comunidad de software de código abierto, por motivos más directamente relacionados con la economía que no con la tecnología.

_ Bernardo Quintero y Jesús Cea acuden de invitados a e-Gallaecia. Hablan de los problemas de las detecciones basadas en firmas y crean en directo un gusano para la ocasión en apenas unas líneas de VBS, para comprobar cómo con simples modificaciones se hacía invisible a los motores antivirus. Era una prueba



de concepto muy básica que no infectó a nadie, y además se envía a los laboratorios antivirus para que la incluyeran en sus firmas. Lo bautizaron como "Galla". Enumeran diferentes estrategias para hacer frente a las limitaciones de la detección por firmas, desde la heurística en el análisis de código hasta la detección genérica basada en el comportamiento. Algo que sería común a partir de 2005. En 2002 nadie había apostado fuerte por esta estrategia de detección basada en el comportamiento como complemento a las firmas. Hispasec presenta entonces su propia prueba de concepto: **SecureCenter**. Creado para la ocasión, básicamente contaba con un monitor de archivos y del registro de Windows, además de alguna opción para configurar automáticamente contra virus algunos aspectos de Windows y Office. La idea era: en vez de reconocer a los virus por una firma que los identifique, reconocerlos de forma genérica por el tipo de acciones que pretenden llevar a cabo en un sistema. El programa fue descartado, aunque suponía un adelanto a las técnicas que más tarde ofrecerían todos los antivirus.

_ Se bautiza con el nombre de **Frethem** un gusano caracterizado por venir en un mensaje con el asunto "Re: Your password!". Alcanza índices de incidencia bastante altos. El virus tiene las mismas características que BadTrans, Nimda o Klez, pero aun así consigue altas cotas de infección. Aprovecha la vulnerabilidad iFRAME del Internet Explorer 5.01 y 5.5 y puede hacer que el usuario se vea infectado sin llegar a abrir el mensaje, puesto que consigue ejecutarse desde las vista previa de mensajes del cliente de correo electrónico Outlook y Outlook Express.

_ Se populariza en los virus el cambio o falsificación de dirección de remitente en los correos. Recibir un mensaje que intenta infectar con el virus del momento no indica expresamente que el remitente mostrado también esté infectado. Los usuarios comienzan a acusar o advertir a los remitentes, creando una preocupación innecesaria. Esto también provoca un aluvión de mensajes automáticos informativos de los antivirus en las pasarelas de correo: primero los del tipo que avisan al supuesto remitente de una falsa infección. Segundo los que avisan al receptor de que una dirección (simulada y que nada tiene que ver con su dueño real) intenta infectarlos. Se crea mucha confusión, acusaciones y mala imagen injustificada entre usuarios y empresas.

Es el año de los **programas troyanizados en servidores oficiales**. En agosto se detecta que la distribución oficial de OpenSSH está troyanizada. El código fuente del paquete OpenSSH es modificado por un intruso y puesto a disposición de todos a través de la página web. Entre el 30 y el 31 de julio se insertó el código de un troyano en las versiones de OpenSSH 3.2.2p1, 3.4p1 y 3.4 sobre el servidor FTP oficial de OpenBSD y de ahí se propagó a través del proceso normal de replicación a otros servidores FTP. Las versiones de OpenSSH afectadas por el troyano contienen un código que permite abrir una shell remota con los permisos del usuario que compiló OpenSSH. Ocurriría lo mismo con Sendmail en octubre de ese mismo año. Un intruso modifica el código fuente para incluir el troyano y compromete la seguridad del servidor FTP oficial para hospedar las copias infectadas. En noviembre, el servidor utilizado para la distribución de dos herramientas muy utilizadas por los profesionales de la seguridad, tcpdump y libpcap, también es atacado para introducir un troyano en el código fuente de estos programas. El troyano consistía en una modificación del archivo de configuración (./configure) y de uno de los archivos de código fuente para

permitir a un atacante tomar el control del sistema afectado en remoto. Por otra parte la modificación efectuada en el código fuente de libpcap es para ignorar todo el tráfico con origen o destino a la puerta trasera.

_ Symantec anuncia la adquisición de cuatro compañías centradas en el mercado de la seguridad: Mountain Wave, Recourse Technologies, Riptech y **SecurityFocus**, por un valor total cercano a los 375 millones de euros. La adquisición del portal SecurityFocus, que hasta el momento gozaba de una gran reputación como portal de información independiente sobre seguridad, levanta una gran polémica. Los niveles de calidad de la página, sin embargo, se mantendrían con el tiempo.

Palladium es el nombre en clave que recibe una iniciativa de Microsoft para implementar la especificación TCPA (Trusted Computing Platform Alliance). Se habla de Palladium como un ambicioso proyecto que supone una revolución en la arquitectura del PC que hoy conocemos. El objetivo final del proyecto Palladium es crear una nueva plataforma informática que mejore ostensiblemente la capacidad de los usuarios para proteger la privacidad de sus datos y controlar el software que se ejecuta en sus máquinas. Microsoft también plantea Palladium como la plataforma para una nueva serie de servicios relacionados con la privacidad, el comercio electrónico y el entretenimiento. Uno de sus objetivos básicos es poner fin al descontrol existente en el mundo de los virus informáticos. Una de las características que más llama la atención es la posibilidad de impedir la ejecución de cualquier código que no esté firmado digitalmente por una fuente de confianza, pero a nivel de hardware. Los defensores del software libre se quejan. Si la nueva versión del núcleo de Linux, por ejemplo, no dispone de una firma digital de una gran compañía, un sistema basado en Palladium se negaría a ejecutarlo. Se crea StopPalladium.org. El proyecto Palladium como tal fracasa y se desvanecería en enero de 2003, pasando a llamarse "Next-Generation Secure Computing Base for Windows" y funcionando de forma mucho más discreta y menos intrusiva de lo imaginado en un principio.

_ En junio, la muerte del responsable de la conservación y archivado de importantes documentos históricos de Noruega los deja inaccesibles. Los documentos se conservaban cifrados, y la única persona que conoce la clave muere sin comunicarla. Ottar Grepstad, director del Centro Nacional de Lenguaje y Cultura de Noruega, realiza un llamamiento mundial solicitando ayuda para atacar el cifrado o sus contraseñas, y así recuperar los documentos. Apenas cinco horas más tarde, un programador sueco envia la clave: **LADEPUJD**. La clave se trata, en realidad, del nombre escrito al revés del propietario original de los archivos. Esa información se indicaba en el dossier publicado con los antecedentes de los archivos, con la esperanza de que proporcionasen alguna pista sobre la clave utilizada. Cientos de usuarios acertarían sin dificultad la respuesta correcta

_ En agosto salta a los medios un **troyano capaz de burlar a los cortafuegos**. Aprovecha Internet Explorer para burlar las protecciones de los firewalls, aunque el concepto no es nuevo y lleva tiempo utilizándose. El troyano, diseñado como prueba de concepto, se da a conocer en la DefCon con el nombre de **Setiri**. La "novedad" que incorpora es que abre una ventana invisible de Internet Explorer y se conecta con un sitio para descargar distintos módulos del troyano, recoger los comandos y enviar información sensible. Los cortafuegos personales que se instalan como software en los mismos sistemas, no detectan nada anormal en Setiri puesto que la transmisión de datos se realiza a través del Internet Explorer, una de las primeras aplicaciones que se marcan como legítimas para conexiones externas en el cortafuegos. Esta

técnica sería, a partir de 2004, usada por la práctica totalidad del malware bancario.

_ **MessageLabs** protagoniza unas vergonzosas declaraciones. Desde la compañía británica se lanzan los siguientes titulares: "Los creadores de virus a través de Internet se convierten en inofensivas reliquias del pasado". "Expertos aseguran que desaparece la amenaza de los virus". Queda la duda de si forma parte de una burda táctica para provocar la creación de nuevos virus o si se trata de un intento desesperado de alcanzar cierta notoriedad en los medios de comunicación. MessageLabs ofrece un servicio antivirus externo para filtrar el correo electrónico. El simulacro de argumento ofrecido por la compañía viene a decir: "Han pasado 18 meses desde que el virus Anna Kournikova, considerado por muchos el último gran virus de ordenadores creado por un precoz programador, infligió graves daños en el mundo corporativo, en lo que podría ser un indicio de que su época ha pasado. Ya no son la amenaza que eran". Mark Toshack, analista de la firma británica de seguridad MessageLabs, se cubriría de gloria.

Dos esfuerzos distribuidos mundiales culminan sus retos con éxito, tras casi cinco años de proceso. El **reto RC5-64** forma parte de un conjunto de retos ofertados por la compañía RSA, con el fin de concienciar a los usuarios sobre la importancia de la criptografía y la resistencia relativa de cada algoritmo según el tamaño de claves. Distributed.net coordina el proyecto. Voluntarios prestan de forma altruista los tiempos "ociosos" de sus máquinas para procesar datos del algoritmo de cifrado elegido. Mediante un sistema distribuido donde son asignados bloques de claves a cada cliente y coordinadas con un servidor, se intenta por fuerza bruta averiguar el mensaje cifrado con un algoritmo concreto. En 1999 se propusieron romper un mensaje cifrado con el algoritmo RC5 de 64 bits por fuerza bruta y en julio de 2002 la clave buscada es encontrada por un PentiumIII a 450Mhz, en Japón. La clave en cuestión es "0x63DE7DC154F4D039", y el texto descifrado se lee como "Some things are better left unread".

Los detalles destacados del reto:

. Se ha mantenido en funcionamiento ininterrumpido durante casi 5 años, aprovechando los recursos puestos a su disposición por cientos de miles de usuarios repartidos por todo el mundo.

. A lo largo del proyecto, se han involucrado en él más de 331.252 personas.

. Hasta encontrar la clave correcta, se comprobaron 15.769.938.165.961.326.592 claves distintas.

. Ha habido días en los que se ha comprobado el 0.12% del espacio de claves. Si ese ritmo se hubiera mantenido durante todo el proyecto, se hubiera encontrado la clave en 790 días, en vez de en 1757.

. Ese ritmo es equivalente a 32.504 Apple PowerBook G4 a 800 MHz o 45.998 AMD Athlon XP a 2 GHz trabajando a la vez.

En noviembre, tras cuatro años, un equipo de la universidad de Notre Dame, en Indiana, supera el **reto ECCp-109**, propuesto por la empresa Certicom en 1997. La criptografía

de curvas elípticas permite la creación de criptosistemas asimétricos (como RSA), pero utilizando curvas elípticas en vez de números primos. Su ventaja fundamental consiste en que las claves son mucho más cortas (160 bits en vez de 1024 bits, por ejemplo) y los requerimientos de memoria y CPU para realizar las operaciones criptográficas son bastante inferiores. Su desventaja fundamental es que muchas de sus variantes están patentadas y no pueden utilizarse de forma libre.

El reto ECCp-109 ofrece un premio de 10.000 dólares a quien consiga descifrar un mensaje cifrado con una clave ECC de 109 bits. El equipo de la universidad de Notre Dame mantuvo 10.000 ordenadores funcionando 24 horas durante 549 días para descifrar el mensaje. Participan más de 247 equipos de todo el mundo, sumando más de 10.308 personas. Certicom patrocina estos retos como una forma de verificar la seguridad de su tecnología, para aumentar el conocimiento de la misma por parte del público y para demostrar la robustez del sistema criptográfico incluso con claves de pequeño tamaño. Comercialmente Certicom utiliza tecnología de 163 bits, lo que resulta unos cien millones de veces más robusta que el reto resuelto.

_ Con la presentación del **Service Pack 1 para Windows XP**, Microsoft pretende que únicamente los usuarios de copias legales del sistema operativo pudieran instalarlo. El resultado es un auténtico fiasco. Cuando se procede a la instalación del Service Pack para Windows XP el programa de instalación realiza una verificación para determinar si el sistema operativo es una copia legítima o pirata. Para ello, se comprueba el número de serie del sistema cotejándolo con una lista negra. Si el número de serie figura dentro de esta lista, no puede realizarse la instalación. Desde entonces, cada vez que un usuario visite el servicio “Windows Update” se procederá a comprobar si su sistema operativo es una versión legítima. Tan pronto como se detecte una versión pirata, Microsoft bloqueará el acceso al servicio automático de actualizaciones aunque se podrá seguir actualizando el sistema a través del servicio de actualizaciones interno. No obstante, y antes de incluso de la disponibilidad oficial del Service Pack, se publicaron en diferentes web métodos que explicaban cómo saltarse esta protección de forma que los usuarios de versiones no legales de Windows XP también pudiesen realizar la instalación del Service Pack.

El 21 de octubre Internet se tambalea. Se realiza un **ataque organizado de denegación de servicio sobre los servidores raíz DNS**. Cada vez que se escribe un nombre, éste debe ser traducido a una dirección IP numérica. Cada ordenador tiene la dirección del servidor de nombres local, habitualmente configurado por el ISP. Si este servidor de nombres local no conoce la conversión a realizar, pasa la solicitud de conversión al servidor responsable del dominio .COM (dominio de primer nivel). En el caso de que no sepa cuál es el servidor responsable del dominio de primer nivel, realiza la consulta a uno de los servidores raíz. Estos servidores raíz disponen de punteros a todos los servidores responsables de los dominios de primer nivel: .com, .net, .org, .es, .uk, .info...

En 2002 existen 13 sistemas considerados servidores raíz en todo el mundo: diez de ellos situados en Estados Unidos, dos en Europa (Londres y Estocolmo) y otro en Japón (muy poco despúes se uniría un decimocuarto servidor raíz situado en España por Espanix). La distribución original deja mucho que desear por su elevada concentración de servidores en áreas geográficas muy reducidas. Durante aproximadamente una hora, entre las 22:45 y las 23:45 CET del 21 de octubre, se detecta un ataque distribuido de denegación de servicio contra todos los servidores raíz. Durante el apogeo del ataque un máximo de siete

servidores raíz tuvieron problemas y se calcula que únicamente un 6% de las peticiones de resolución no fueron atendidas. Lo más significativo de este ataque fue que tenía como objetivo todos los servidores raíz, de forma simultánea.

Con anterioridad han existido algunos problemas con la resolución de nombres con un impacto mayor. En abril de 1997 el sistema de resolución de nombres no funcionó durante varías horas debido a que un router, por error en su configuración, se anunció él mismo a todos en Internet como el camino más rápido para acceder a otras direcciones. Esto causó que todas las peticiones intentaran utilizar este servidor, provocando el colapso de la red.

_ En 2002 se superan los **40.000 suscritos** directamente por correo a una-al-día. En 2008 son más de 35.000 los suscritos directamente por correo y se diversifican las fuentes de lectura con canales alternativos como el RSS.

_ En diciembre, **eBay**, la mayor casa de subastas del mundo, comunica que sus 55 millones de clientes está en el punto de mira de un **espectacular fraude** al que todavía no se le daría el nombre de "phishing". En 2008, eBay y PayPal siguen siendo las favoritas indiscutibles de este tipo de estafas.

_ Tras más de 5 años sin cambios, se publica una **actualización de la zona raíz** del sistema DNS.

Una al día

01/01/2002 Gusanos de Internet: pasado, presente y futuro (III)

En la última entrega de esta trilogía sobre gusanos de Internet vamos a abordar que nos puede deparar el futuro más inmediato en el terreno de los códigos víricos. Hablar de futuro en el mundillo de los virus supone un ejercicio de responsabilidad, ya no tanto por el grado de acierto que se pueda tener, de cara a la galería, entre las ideas expuestas y lo que finalmente suceda, sino por la posibilidad de que algún comentario resulte ser original y se convierta en la semilla de algún nuevo virus.

En este sentido recuerdo que dejé de escribir un artículo, durante los primeros años de Windows 95 y la generalización de Internet, sobre el peligro que entrañaría el desarrollo de un gusano que explotara la compartición de recursos aprovechando que Windows 95 "montaba" por defecto NetBIOS sobre TCP/IP. El resultado era que las máquinas que compartían sus recursos en una red local, como puede ser un disco duro, también lo hacían automáticamente para cualquier usuario de Internet.

Por aquel entonces era un agujero de seguridad muy generalizado, que Microsoft nunca reconoció como tal y por tanto no existía aviso ni parche oficial, de forma que escanear de forma arbitraria una clase C en Internet devolvía la mayoría de las veces algunas máquinas con este grave problema donde no faltaban las que compartían todo el disco duro. Que el gusano realizara una copia de si mismo en la carpeta de Inicio de Windows en el disco duro remoto no era empresa difícil, de forma que la próxima vez que se iniciara Windows el virus se ejecutaría automáticamente y procedería a buscar nuevas víctimas una vez conectado a Internet. Por fortuna, nunca sabremos el impacto que un gusano de este tipo pudo haber causado en aquellas circunstancias.

La verdad es que aquellos años los creadores de virus estaban más ocupados investigando a fondo los entresijos de Windows 95 para poder crear virus compatibles con el nuevo sistema y formato de ejecutables. Se abría un periodo de adaptación para trasladar y adaptar todas las técnicas que habían venido utilizando hasta la fecha en la antigua escuela aprovechando todo los recovecos del DOS. No perdieron el tiempo, la innovación en el terreno de los virus Win32 ha sido constante, con la incorporación de nuevas técnicas que nunca llegamos a imaginar.

De un modo u otro, lo que está claro es que Microsoft juega un papel fundamental en el terreno de los virus informáticos. Dejando a un lado que por diseño sus sistemas sean más o menos seguros y que faciliten en parte la vida a los virus, su importancia viene de la posición predominante que ocupa en el mercado de los sistemas operativos, aplastante en el caso de los usuarios domésticos y puestos clientes. Si el fin de un virus es sobrevivir y reproducirse al máximo, lo normal es que se diseñe para que pueda afectar al mayor número de víctimas posibles, y hoy día en el caso de la informática eso se traduce en la compatibilidad con Windows y productos Microsoft.

Además de los virus para DOS y la nueva generación Windows ya comentada, la historia deja claro que la aparición de nuevas clases o familias de virus se basa en los nuevos productos o tecnologías Microsoft. Si con Office asistimos al nacimiento de la plaga de los virus de macro, con gusanos como “Melissa”, la incorporación por defecto del interprete Windows Scripting Host en Windows 98 y posteriores nos trajo el aluvión de gusanos escritos en Visual Basic Script (VBS), como “ILoveYou” y compañía.

Visto ésto, para hablar de futuro en el mundo de los virus informáticos, que mejor que darse una vuelta por la web de Microsoft para ver las nuevas tecnologías y productos que con casi total seguridad terminarán implantándose de forma global.

Tanto si visitamos www.microsoft.com, como si somos asiduos a las noticias de tecnología, veremos que Microsoft ha puesto mucho hincapié en introducirnos a su nueva tecnología .NET, que se hará notar tanto en los sistemas operativos como en las aplicaciones. .NET nos abrirá la puerta a la informática distribuida con nuevas funcionalidades que facilitarán la conexión de componentes a través de redes, un ambiente que a buen seguro aprovecharán los creadores de virus.

Si profundizamos en .NET, en lo que desarrollo se refiere, podemos ver nuevos conceptos como el Common Language Runtime, un modelo que busca integrar el código generado por los compiladores de manera independiente al lenguaje utilizado. Para lograrlo aparece un nuevo lenguaje y su correspondiente formato de archivo, Microsoft intermediate language (MSIL), que además amenaza con que su código es independiente al juego de instrucciones de la CPU, en su búsqueda por convertirse en un estándar que termine por implantarse también en otras plataformas. El sueño de cualquier creador de virus, un formato que le permita de forma fácil diseñar gusanos multiplataforma.

En futuras entregas, fuera de esta trilogía, abordaremos algunas funcionalidades y características de .NET y las implicaciones que pueda tener en la seguridad de nuestros sistemas. De momento nos quedamos con .NET y MSIL (Microsoft intermediate language) como candidatos a caldo de cultivo para una nueva generación de virus y gusanos.

Bernardo Quintero

04/04/2002 La trastienda del "full disclosure"

Las últimas vulnerabilidades publicadas por Guninski, antes de que Microsoft proporcione los correspondientes parches, reaviva el recurrente y cansino debate sobre la divulgación total en materia de seguridad informática ("full disclosure").
Posturas iniciales

A grandes rasgos la discusión se presenta bastante simple y obvia, al menos en su vertiente de cara a la galería. Por un lado nos encontramos con las casas de software, que argumentan que la publicación de detalles sobre nuevas vulnerabilidades es contraproducente para la seguridad, ya que facilita la labor a los potenciales atacantes.

En frente, investigadores independientes, criptólogos, hackers y grupos de seguridad informática, entre otros, que consideran que la información debe ser libre y divulgada a la opinión pública. Bajo su prisma, el conocimiento permite establecer defensas contra unos ataques cuyos detalles circularían en cualquier caso entre los atacantes, puesto que el "underground" mantiene canales de comunicación sobre los que no es posible ejercer ningún tipo de control.

Situación actual

Existe un código no escrito de buenas maneras que establece que, antes de realizar cualquier aviso público, el hacker o investigador debe poner en sobreaviso a la empresa afectada, proporcionándole todos los detalles sobre las vulnerabilidades que ha descubierto en cualquiera de sus productos y, en la medida de lo posible, ayudando en su resolución.

Esta regla suele cumplirse en la inmensa mayoría de los casos, si bien no está exenta de problemas y contratiempos. En ocasiones resulta toda una odisea poder, simplemente, hacer llegar la información a la persona adecuada y/o recibir un acuse de recibo. Por contra, y a favor de las empresas, hay que decir que algunas cuentan con direcciones y personal dedicado exclusivamente a este menester, como es el caso de Microsoft. En otros casos, aun habiendo existido contacto entre descubridor de la vulnerabilidad y desarrollador afectado, no hay un acuerdo en la importancia del problema o en la urgencia y tiempos de resolución que requiere.

Este tipo de contratiempos suelen acabar con la publicación prematura de los detalles de las vulnerabilidades y medidas preventivas de carácter urgente propuestas por el descubridor, antes de que los desarrolladores hayan facilitado un parche o aviso oficial.

En estos casos el descubridor argumenta que se ha visto obligado a la publicación para poner en aviso a los usuarios afectados ante un problema que considera puede afectarles, a la vez que espera que la presión pública fuerce a la empresa a una rápida actuación y resolución de la vulnerabilidad.

Por su parte, los desarrolladores se quejan de que el proceso de análisis de la vulnerabilidad, diseño del parche, y posteriores comprobaciones y tests de calidad, no es tarea fácil y requiere más tiempo, de cara a facilitar al usuario final una solución fiable y segura.

Lo que la verdad esconde

Como vemos, tanto unos como otros, utilizan como excusa de sus argumentos la seguridad del usuario. Parece ilógico que teniendo un mismo fin no se pongan de acuerdo. En realidad, como cabe pensar, existen

otros intereses más partidistas y lucrativos en juego.

La imagen, y todo lo que se deriva de ella, es realmente uno de los principales factores que originan el debate "full disclosure". El anuncio público de una nueva vulnerabilidad, con sus respectivos ecos en sitios especializados y, cada vez más, en otros medios de comunicación, lleva consigo un aumento de popularidad y publicidad para el descubridor, mientras que para la empresa supone un duro varapalo para su producto e imagen corporativa. En algunos casos concretos cabe pensar que este es el interés que prima, de otro modo costaría entender determinadas actitudes por ambas partes.

¿Qué opción es la correcta?

En mi opinión personal, si buscamos la seguridad de los posibles usuarios afectados, no existe una única vía de actuación, no hay que se extremistas en uno u otro sentido.

Por ejemplo, pasando por avisar en primer lugar a la empresa del producto vulnerable, tal vez creamos conveniente dar un aviso con algunas indicaciones para que los usuarios puedan tomar medidas preventivas mientras se desarrolla el parche, si bien no tiene mucha razón de ser dar todos los detalles de forma explícita o adjuntar código de ejemplo durante esta fase.

Los problemas se presentan bien cuando el descubridor lanza los detalles sin avisar a la empresa, bien si la empresa hace caso omiso del aviso o no presta la atención que la vulnerabilidad se merece. En condiciones normales, si existe ánimo de cooperación por ambas partes, no tienen porqué existir conflictos de intereses.

Bernardo Quintero

25/04/2002 ¿Infectado por "Klez.x"? Hora de cambiar de antivirus

La última variante del gusano "Klez" está causando furor desde la semana pasada, alcanzando unas cifras de infecciones muy significativas. Antes de que viera la luz esta nueva versión ya existían técnicas para detectarlo de forma genérica, sin necesidad de actualizaciones de última hora. Si aun teniendo un antivirus se vió infectado por "Klez.x" de forma automática, tal vez sea hora de plantearse un cambio de producto. Puede llamar la atención de algunos lectores la "x" que he utilizado en el "apellido" de esta versión de "Klez", pero ante la diversidad de criterio de las casas antivirus, en lo que a nomenclatura se refiere, he preferido no decantarme por ninguna de las letras utilizadas. Es decir, cambie la "x" por "G", "H", "I" o "K", al fin y al cabo, el nombre es lo de menos.

Aunque a día de hoy cualquier antivirus actualizado lo detecta, no sucedió lo mismo en los primeros momentos de propagación, como suele ocurrir cuando aparece un virus de nueva creación o variante. Dejando a un lado la detección heurística, capaz de lo mejor y lo peor, existe una forma muy fácil de reconocer e impedir la acción de este tipo de gusanos.

¿Qué tienen en común, entre otros, gusanos tan extendidos como BadTrans, Nimda o el propio Klez.x? Todos aprovechan vulnerabilidades para forzar la ejecución, y por tanto infección, automática, sin necesidad de que el usuario abra o ejecute un archivo, sin duda la característica que los ha dotado de mayor poder de propagación.

Más curioso aun resulta que los tres gusanos nombrados, protagonistas de verdaderas epidemias, explotan la misma vulnerabilidad para forzar la ejecución automática en el cliente de correo Outlook Express (Nimda, además de ésta, aprovecha otras vulnerabilidades para infectar servidores IIS).

La cosa se agrava si tenemos en cuenta que la vulnerabilidad en cuestión data de marzo de 2001, y que es muy fácil de detectar analizando el mensaje de correo electrónico. Basta con mirar si una cabecera MIME hace referencia a un programa ejecutable que simula ser un formato confiable, por ejemplo un archivo de audio.

Aunque para los menos iniciados pueda sonar complicado, vamos a ver algunos ejemplos reales de las cabeceras utilizadas por estos gusanos para comprobar los elementos comunes, lo que convierte en trivial su detección por cualquier antivirus para clientes, e incluso a través de un sencillo filtro en el servidor de correo:

BadTrans-> Content-Type: audio/x-wav;
name=”news_doc.DOC.scr”
Nimda-> Content-Type: audio/x-wav;
name=”readme.exe”

Klez.x -> Content-Type: audio/x-wav;
name=200).exe

En definitiva, desde marzo de 2001 todos los antivirus podrían haber detectado de forma genérica cualquier e-mail donde viaje un gusano que intenta explotar esta vulnerabilidad del Outlook Express, para lograr la ejecución de forma automática. Lo fácil de su detección y lo crucial que resulta para la seguridad del usuario convierten a este tipo de detección de ataques o “exploits” en un requisito exigible e imprescindible en un buen antivirus.

Hay que decir que algún que otro antivirus ya cuentan con este tipo de detecciones, sólo cabe esperar que no detecten esta noticia como un gusano o intento de exploit por contener los anteriores ejemplos. Si bien, dejaremos la problemática de los falsos positivos para otra entrega.

Bernardo Quintero

15/05/2002 “Spam” para robar datos sensibles

Todos los usuarios de Internet hemos recibido en alguna ocasión mensajes de correo electrónico no solicitados de alguien que no conocíamos, la mayoría de las veces con anuncios y publicidad. Este tipo de mensajes enviados de forma masiva e indiscriminada es lo que denominamos “correo basura” o “spam”. En los últimos tiempos hemos podido observar como prolifera esta vía para hacer llegar mensajes que, mediante engaños, tratan de robar información sensible del usuario, como contraseñas y datos de tarjetas de crédito.

Curiosidades

Debemos retroceder a 1926 para encontrar el término “Spam”, que en su origen hacía referencia al

jamón con especias (Spiced Ham) de la casa Hormel, primer producto de carne enlatada que no requería refrigeración. Esta característica convirtió al "Spam" en un producto muy extendido, que podía encontrarse en cualquier parte.

Además de ser utilizado en la segunda guerra mundial por los ejércitos como parte imprescindible de los víveres, el "Spam" solía acompañar a cualquier plato de la cocina americana de la época. La popularidad que ha alcanzado este producto es tal que hoy día podemos visitar hasta su propio museo. El uso masivo que se hacía del "Spam", que podía encontrarse prácticamente en cualquier sitio, puede ser la razón por la que se ha utilizado este término para calificar el envío de correo indiscriminado a través de Internet.

También basándose en el producto de carne enlatada, algunos defienden que el uso del término "spam" para calificar al correo basura se popularizó a raíz de una obra de los británicos Monthy Phyton en una escena en la que en un restaurante todos los platos eran acompañados por "spam". Otra teoría alternativa afirma que el término SPAM es el acrónimo de "Stuff Posing As Mail", traducido como "mentira que se presenta como correo".

En el ataque

La versatilidad del correo electrónico a través de Internet, como toda tecnología, puede utilizarse con distintos fines. Hace apenas una semana se ha distribuido un "spam" masivo que bajo el asunto "An Urgent notice from eBay Safe Harbor !", simulaba ser un aviso a los usuarios registrados del popular sitio eBay. El mensaje fraudulento notifica que los datos de nuestra cuenta de eBay deben ser actualizados por encontrarse erróneos o corruptos, para lo cual facilita un enlace a un formulario web que deberemos rellenar para que no se nos interrumpa el servicio.

Para darle más credibilidad, la dirección de remite aparece como "Safe Harbor" <SafeHarbor@eBay.com>, mientras que a lo largo del mensaje hace referencia a que se utiliza SSL para que los datos transferidos viajen de forma segura, así como todo tipo de garantías sobre privacidad avalada por terceros. Una vez llegamos al formulario, mediante una URL encabezada por la IP del servidor, para intentar ocultar que el dominio no pertenece en realidad a eBay, nos encontramos con el citado formulario que simula el interfaz de eBay (logos, etc).

Por descontado, toda la información que se introduzca llegará a las manos del atacante, que podrá utilizarla para suplantar la identidad de los usuarios de eBay o realizar compras en otros sitios con los datos de sus tarjetas de crédito.

Bernardo Quintero

24/07/2002 Certificaciones antivirus obsoletas

Ancladas en el pasado, las principales certificaciones antivirus como ICSALabs, Checkmark o VB 100%, no se ajustan a las necesidades actuales de los usuarios ni evaluan en su justa medida la realidad de las soluciones antivirus de hoy día. Sus logotipos suelen ocupar contraportada de las cajas de productos y aparecen en las webs de las casas antivirus como galardones que, supuestamente, certifican la calidad de sus soluciones. Si nos adentramos un poco en sus especificaciones encontramos que los tests son pobres y se centran principalmente en los porcentajes de detección, y en el mejor de los casos desinfección, sobre colecciones de muestras conocidas.

Con la explosión del fenómeno Internet, y las implicaciones que todos conocemos en el mundo de los virus informáticos, sobre todo a modo de i-worms, el modelo reactivo de los antivirus tradicionales, basados en ofrecer vacunas después de haber detectado un espécimen nuevo, deja de ser una solución efectiva.

En el tiempo en que se detecta un virus nuevo, es analizado por el laboratorio antivirus, desarrollan la vacuna, la solución pasa el control de calidad interno, ponen la nueva firma de detección a disposición de los usuarios y éstos se actualizan, un gusano de Internet o i-worm puede haber infectado miles y miles de sistemas. No hay que incidir mucho en esta cuestión, basta con nombrar a "Melissa", "ILoveYou", "Kournikova", "Nimda", "BadTrans", "Sircam" o "Klez", entre otros muchos.

En este punto alguien podría preguntar por las heurísticas actuales, ya que supuestamente, o al menos así se venden, son las tecnologías encargadas de detectar nuevos virus. Queda claro por la experiencia que no son efectivas, de lo contrario no tendríamos que recordar para nada los nombres de especímenes antes comentados.

Las heurísticas, en realidad, son también detecciones basadas en firmas, pero que buscan porciones de código más genéricas en vez de la cadena concreta que identifica a un virus en particular. El diseño de un virus nuevo, o la ofuscación a nivel de código de uno ya existente, burla de forma trivial este tipo de detección. Una pequeña prueba de concepto se pudo ver el pasado junio durante las jornadas de seguridad de e-Gallaecia, donde mi compañero Jesús Cea y yo expusimos sobre las debilidades de las soluciones antivirus actuales. El simple uso de variables intermedias, en un gusano escrito en Visual Basic Script de apenas 20 líneas de código, logró vencer a las heurísticas de los principales productos antivirus del mercado.

El futuro, que ya debería ser presente, pasa claramente por la implantación de tecnologías proactivas capaces de ofrecer al usuario sistemas de protección contra virus nuevos sin necesidad de recurrir a continuas actualizaciones. Claro está que no es la panacea, no acabará con la problemática de los virus, y seguirán siendo necesarias las actualizaciones puntuales, pero la capacidad de prevención de las soluciones antivirus aumentará drásticamente y el usuario dejará de tener la sensación de indefensión total durante las primeras horas de propagación de un virus nuevo.

Las buenas noticias son que algunas casas antivirus, bien por exigencias del mercado, bien por convencimiento propio o como ventaja competitiva, ya comienzan a implantar funcionalidades proactivas que van más allá del antivirus tradicional que todos conocemos.

Volviendo al títular que nos ocupa, el problema es que estas nuevas tecnologías no son evaluadas por las certificaciones actuales, cuyas metodologías sólo se centran en la detección a nivel de código. El resultado es que hoy día algunos productos antivirus pueden llegar a ser incluso penalizados en este tipo de evaluaciones, cuando en realidad el nivel de protección que ofrecen es muy superior al de otras soluciones que simplemente, al igual que las certificaciones, se han quedado ancladas en el pasado.

Bernardo Quintero

13/08/2002 Antivirus corporativo: dos (diferentes) mejor que uno

Aunque el titular parece obvio, "dos mejor que uno", la realidad es que la mayoría de las corporaciones terminan instalando en sus sistemas, tanto servidores perimetrales como estaciones de trabajo, la misma

marca antivirus, lo que penaliza la capacidad de detección. Desde Hispasec Sistemas, en nuestra faceta de consultores y de manera independiente a la publicación de la comparativa antivirus anual para PCs, realizamos análisis a demanda de cara a presentar proyectos sobre la implantación idónea de soluciones antivirus según un determinado entorno corporativo. Desde esta experiencia, y en virtud de la situación de partida con la que nos encontramos en cada caso, hemos podido observar que la mayoría de las corporaciones suelen contratar con una sola casa antivirus la protección de todos sus sistemas. Situación que solemos corregir.

Aunque las casas antivirus suelen tener una amplia gama de soluciones según el puesto a proteger, la realidad es que todos sus productos comparten el mismo motor antivirus y base de datos de firmas. Es decir, si instalamos en el firewall, el proxy, el servidor de correo, en el servidor de ficheros, y en las estaciones de trabajo el antivirus de la marca X, habremos aumentado cuantitativamente el número de chequeos, pero no su calidad.

Imaginemos que queremos proteger un edificio y situamos un guarda jurado o personal de seguridad en la puerta del garaje, otro en la entrada del edificio, uno más en la puerta de los ascensores, y por último repartimos varios guardas en la puerta de cada una de las oficinas. Todos se han formado de la misma forma y siguen las mismas pautas de actuación, además todos tienen la misma lista de intrusos sospechosos basándonos en fotografías de sus rostros.

Cada persona que quiere acceder al edificio es examinada por varios de los guardas dependiendo de la vía de entrada que utilice, pero en todos los casos la comprobación es la misma. Si un intruso no aparece en la lista de sospechosos, podrá burlar a todos los guardas de manera independiente a la vía que haya elegido para entrar (virus nuevo no reconocido).

Otro caso que puede darse es que un intruso ya fichado intente disfrazarse para burlar a los agentes. Si todos los agentes siguen las mismas técnicas de reconocimiento (motor antivirus), como por ejemplo pedir que se quiten las gafas de sol en caso de duda, el intruso podrá pasar inadvertido empleando otras técnicas de camuflaje, por ejemplo utilizar una peluca (variante o nueva versión de un virus conocido).

Parece obvio que lo ideal sería contar con varias listas de sospechosos y guardas con diferentes capacidades y métodos de reconocimiento de forma que se puedan complementar entre sí, aumentando el grado de protección global. Siguiendo la analogía con los antivirus, cada motor tiene sus características y bases de datos de firmas diferentes que se actualizan de manera independiente.

La realidad es que no basta simplemente con incluir más de un motor antivirus, ya que se hace necesario un estudio sobre el grado de complementariedad entre los distintos motores, el rendimiento y estabilidad que ofrecen según el puesto de la red, y facilitar la gestión y administración centralizada de los productos elegidos según la casuística.

Bernardo Quintero

31/10/2002 Comentarios sobre los antivirus perimetrales

Siendo el correo electrónico el principal medio de propagación e infección de virus informáticos y gusanos, parece lógica la implantación de sistemas antivirus a nivel de servidores de correo, así como en otros puntos críticos de la red, por ejemplo un proxy, por donde se canalizan las conexiones de los usuarios corporativos a Internet.

No obstante la implantación de estos sistemas antivirus no está exenta de problemas, en especial a nivel de rendimiento cuando se trata de servidores que manejan un gran volumen de tráfico. Si un usuario es capaz de notar que su PC se enlentece o se vuelve inestable al instalar determinado producto antivirus, el caso se complica aun más cuando hablamos de un servicio tan crítico para la empresa como es el correo electrónico. A buen seguro son muchos los sufridos administradores de sistemas los que pueden contarnos más de una batallita en este sentido.

Para contrarrestar este tipo de efectos, o como causa de ellos, algunos sistemas antivirus hace dejación de sus funciones. Así, por ejemplo, en algunos casos nos hemos podido encontrar con sistemas que dejan de analizar mensajes de forma arbitraria cuando hay mucha carga de trabajo, o aquellos otros que para aumentar su velocidad de análisis no soportan ciertos formatos de empaquetado o la mayoría de formatos de compresión, lo que abre en ambos casos una ventana a la entrada de e-mails infectados.

Aunque los avances son constantes en este terreno, siendo muchos los servidores de correo que ya incorporan interfaces específicos para facilitar la función a los antivirus, la propia naturaleza de los antivirus los penaliza. Esto es así ya que cada día que pasa aumenta la base de datos de firmas que tienen que contrastar para identificar a los virus, así como aumenta las formas y formatos en que éstos pueden ocultarse y presentarse.

También por la propia funcionalidad de los virus y gusanos tradicionales (dejando a un lado los gusanos para servidores web y similares), la capacidad de detección los antivirus, sobre todo a nivel de heurística y proactividad, siempre será menor en un servidor perimetral que en una estación de trabajo o PC. No en vano, el servidor perimetral no deja de ser un punto de tránsito para el virus, mientras que se desenmascara y procede a la infección y resto de acciones en la estación de trabajo, por lo que es más fácil detectarlo en esta última.

Para terminar de poner trabas a los antivirus perimetrales, tampoco hay que pasar por alto que son muchos los casos donde se instala la misma marca de antivirus en todos los puntos de la red, tanto en servidores perimetrales como en las estaciones de trabajo, fruto de "paquetes oferta" o recomendaciones del distribuidor. En estos casos se está multiplicando el número de análisis que se realizan sobre los contenidos que llegan a la empresa, pero no su calidad, ya que las soluciones de la misma marca comparten el fichero de firmas de virus reconocidos. Si un virus es identificado en el servidor de correo, también lo sería en la estación de trabajo, y si burla uno de los puntos probablemente lo hará con el resto. (Antivirus corporativo: dos (diferentes) mejor que uno. http://www.hispasec.com/unaaldia.asp?id=1388).

Llegados a este punto hay que decir que las soluciones antivirus perimetrales son recomendables, se trata de una capa más de protección. Aunque queda claro que están lejos de ser la panacea, y que su implantación requiere un análisis concienzudo que comprenda una comparativa de productos con diversos tests sobre la casuística particular del entorno corporativo donde se ha de instalar. En algunos casos especiales su instalación puede ser no recomendable, y en su lugar será más fácil y adecuado, y no por ello menos efectivo, implantar una política especial de filtros a nivel de contenidos.

Por último, recomendamos que su implantación sea transparente al usuario y que se haga hincapié en la necesidad de no bajar la guardia a nivel de estaciones de trabajo, ya que en muchas ocasiones el saber que existe un antivirus perimetral puede crear una falsa sensación de seguridad, que conlleva el descuidar las prácticas más básicas de prevención.

Bernardo Quintero

11/11/2002 Certificaciones de productos, ¿garantía de seguridad o marketing?

La reciente certificación "Common Criteria" otorgada a Windows 2000 desata la polémica sobre cual es el alcance real de estos galardones sobre la seguridad final de los usuarios.

Las certificaciones, básicamente, son un procedimiento por el cual una parte, en principio imparcial, asegura que un producto, proceso o servicio cumple con una serie de puntos bien definidos. Partiendo de esta base los beneficiarios de esa certificación serían tanto los proveedores, como demostración ante terceros del cumplimiento de una serie de requisitos, así como los clientes, que cuentan con una evaluación independiente que asegura que no les dan gato por liebre, una especie de "control de calidad". Hasta aquí todo bien.

Mi visión sobre las certificaciones es bastante más crítica, en parte formada por los contrasentidos que regularmente me encuentro entre los galardones que ofrecen la mayoría de certificaciones antivirus y los resultados que obtenemos en los tests que realizamos a esos mismos productos durante los análisis y comparativas en Hispasec. Aunque hay muchos matices a discutir, básicamente podríamos resumir en que la metodología utilizada y los requisitos que se exigen en las certificaciones no se ajustan a las necesidades reales de los usuarios y, por tanto, no aseguran un nivel adecuado de protección.

A partir de aquí para mí desaparece el concepto de "calidad" asociado a las certificaciones, que pasan a ser simplemente la confirmación de que un producto, en un determinado momento y bajo unas circunstancias muy concretas, cumple un determinado número de requisitos. La certificación no me asegura que los requisitos evaluados cubran mis necesidades, ni que las circunstancias especiales en las que se cumplen dichos requisitos se den en mi entorno real, ni me puede garantizar que el producto en su próxima actualización siga cumpliendo esos mismos requisitos, y mucho menos puede asegurar (de hecho es más que probable que ocurra) que dentro de x semanas no se descubra una nueva vulnerabilidad crítica que ponga en entredicho no ya al producto, sino incluso a la propia certificación.

En estos momentos todo el mundo recuerda cuando a Windows NT le otorgaron el nivel de seguridad C2, de acuerdo con los estándares de seguridad del Departamento de Defensa de Estados Unidos según el criterio del famoso libro naranja. Entre los "detalles" nos encontramos que la certificación la obtenía un sistema Windows NT sin conexión alguna de red, de lo contrario dejaba de ser seguro. ¿Cuántos sistemas Windows NT se instalan para que funcionen de forma aislada?. Por lo demás, no vamos a enumerar las vulnerabilidades que se descubrieron a posteriori y que afectaban de lleno a los requisitos del nivel C2 (aun estando el sistema sin conexiones de red).

En el caso de la certificación "Common Criteria" recientemente otorgada a Windows 2000, de la que nos hacíamos eco en la anterior entrega de "una-al-día", comparto con mi compañero Xavier Caballé en que se trata de una muestra más del interés que está mostrando Microsoft por la seguridad y, sobre todo, del interés en explotarla como herramienta de marketing, que en mi opinión es la auténtica funcionalidad que tienen las certificaciones para los productos evaluados.

Con esto no quiero criticar a Microsoft, realmente pienso que está consiguiendo adelantos en materia de seguridad en sus productos. Para llegar a esta conclusión, más que fijarme, o fiarme, de los anuncios de galardones, prefiero observar detalles más mundanos que nos afectan a diario a todos como, por ejemplo, que su nueva política de distribuir actualizaciones acumulativas está disminuyendo los riesgos de sufrir regresiones en las vulnerabilidades así como la omisión de parches específicos.

En definitiva, la obtención de certificaciones por parte de productos es un indicador positivo, si bien no

garantizan su seguridad global ni la adecuación a nuestro entorno y necesidades reales. La seguridad es un proceso constante que no debe ser medido puntualmente y de forma aislada.

Bernardo Quintero

30/12/2002 Actualizaciones de Microsoft, un arma de doble filo

A principios de 2002 se presentaba en España, bajo el nombre de Strategic Technology Protection Program (STPP), la iniciativa de Microsoft para mejorar la seguridad de sus productos. Tras la experiencia acumulada en estos últimos meses podríamos resumirla en una sola palabra: automatización.

Bajo el título de “Microsoft STPP, ¿estrategia tecnológica o lavado de cara?”, intenté por aquel entonces balancear entre los pros y los contras de la iniciativa, con un pequeño listado de problemas por resolver que Microsoft arrastraba y que entendía eran críticos (http://www.hispasec.com/unaaldia.asp?id=1213).

En la situación actual, tras casi un año de STPP, parte de esos problemas se han minimizado, otros se agravan, y surgen nuevas interrogantes.

El usuario final mejora su seguridad.

Queda claro que Microsoft ha puesto especial empeño en facilitar la vida a los usuarios automatizando todo el proceso de actualizaciones, tanto en el ámbito de notificaciones, descarga e instalación. Parece que nos dirige hacía sistemas totalmente autosuficientes y transparentes, que se encargarán por nosotros de estar actualizados puntualmente.

Este planteamiento, que ya se intuía con servicios como Windows Update y que se hacen más evidentes en sistemas como Windows XP, corrige en gran parte los problemas de regresión de vulnerabilidades de antaño, al menos los inducidos directamente por el usuario. Básicamente, estos problemas aparecían por la instalación de parches específicos sin el orden adecuado, lo que llevaba a sobrescribir bibliotecas y componentes con versiones más antiguas y, por tanto, la aparición de vulnerabilidades anteriores. Con los nuevos servicios de actualización automática, como Windows Update, es el propio sistema el que decide que parches y en que orden deben ser instalados, minimizando este riesgo.

Por contra, esta misma automatización, agrava el enmascaramiento de nuevas versiones y funcionalidades con la excusa de la seguridad, lo que en algunos casos ha supuesto la aparición de nuevas vulnerabilidades. Lo ideal es que cada vulnerabilidad cuente con un parche específico diseñado para corregirla. Sin embargo, Microsoft suele ofrecer como solución la actualización a nuevas versiones del software o componente afectado, algunas veces de forma pública, y otras veces ocultando las nuevas funcionalidades o modificaciones en un parche de seguridad.

Las implicaciones de esta política en el ámbito de seguridad son varias, por un lado las nuevas funcionalidades incorporadas en los parches o nuevas versiones son en muchos casos origen de nuevas vulnerabilidades, problemas que no habrían aparecido en los componentes anteriores si se hubieran limitado a corregir la vulnerabilidad. Por otro lado, esta práctica es la que provoca la mayoría de incompatibilidades o mal funcionamiento del sistema con el hardware / software ya existente tras haber realizado una actualización de seguridad.

En líneas generales, en lo que respecta al usuario final y balanceando lo dicho anteriormente, la iniciativa STPP representa un avance significativo, ya que ha mejorado los tiempos de actualización de los PCS y facilita en gran manera la tarea al usuario.

Pérdida de control por parte de los administradores y profesionales

Sin embargo, desde el punto de vista de los administradores de sistemas y profesionales, tanta automatización y abstracción se traducen en un menor control, que ya de por sí era bastante limitado en plataformas Microsoft.

De entrada, tanta actualización automática seguro que pone en alerta a más de un administrador de sistemas, que ya habrá experimentado como un simple parche a demanda, o el Service Pack de turno, ha podido volver inestable ciertos servicios, cuando no a todo un servidor. Con esta experiencia, no es de extrañar que algunas políticas corporativas contemplen tests de los parches en equipos de pruebas, durante al menos un mes, antes de pasarlos a los sistemas de producción.

Con STPP se plantean nuevos problemas, ya que Microsoft está optando en muchas ocasiones por "macro parches" acumulativos, que resuelven múltiples vulnerabilidades con una sola actualización. Mientras antes un administrador de sistemas podía decidir si instalar un parche específico o retrasarlo, dependiendo de sí afectaba a la configuración de su servidor o si podía prevenirlo por su cuenta (por ejemplo con reglas en el firewall o modificando la configuración del sistema), ahora esa opción es muy limitada, por lo que tendremos que instalar los "macro parches" aun a sabiendas de que algunas correcciones no las necesitaba nuestro sistema, con las implicaciones que ello pueda acarrear en cuanto a estabilidad.

Por otro lado, la tendencia parece que apunta a que cada vez más los sistemas de Microsoft realizarán operaciones y actualizaciones automáticas, transparentes al usuario, dependiendo de conexiones externas vía Internet. Algunas de estas tendencias ya pueden verse en los sistemas de actualización automáticos actuales o en Windows XP, sin entrar en otras consideraciones como pueden ser el control que Microsoft puede establecer a través de estas vías, políticas de control de licencias o fidelización (sólo permitir actualizar a los usuarios suscritos) y sus implicaciones en el ámbito de la privacidad. Si extrapolamos esto a un servidor, los administradores de sistemas tendrán aun menos control o, dicho de otra forma, contarán con un "superusuario" por encima de ellos: Microsoft.

Windows NT, crónica de una muerte anunciada

Ante este panorama algunos podrían decidir no migrar hacia los nuevos sistemas de Microsoft y quedarse con plataformas como por ejemplo Windows NT, sistemas con años en producción, bien conocidos por los administradores, con múltiples Service Packs a sus espaldas que han ido puliendo sus defectos y mejorándolo, que ya se encuentran bien implantados, cumplen su cometido y no necesitan de las nuevas funcionalidades que propone Microsoft.

Desgraciadamente Windows NT tiene sus días contados, y eso es fácil de predecir, bien observando la historia reciente de Microsoft, bien dejándose llevar por simples reglas de mercado: hay que vender los nuevos productos. En este apartado la seguridad juega un papel crítico, incluso como herramienta para forzar a la actualización. Igual que no hay solución para ciertos problemas de seguridad en Windows 95 o en Internet Explorer 5.0, obligando al usuario a actualizar a Windows 98 o IE6.0 si quiere estar seguro. Es sólo cuestión de tiempo que Microsoft deje de dar soporte a Windows NT.

Posibles mejoras

Desde el punto de vista del administrador de sistemas lo ideal sería ofrecerles la posibilidad de obtener un mayor control. Aunque las comparaciones en este ámbito son casi inevitables, evitaré entrar en el eterno debate entre la comunidad Open Source y Microsoft, no en vano algunas posturas que se podrían copiar y adoptar pueden sonar a pura quimera. Así que las peticiones serán escasas y simples.

De entrada sería importante que Microsoft, además de los macro parches acumulativos, ofreciera la posibilidad de obtener parches específicos e individuales, de forma que el administrador pudiera optar por una instalación personalizada de los mismos, según configuración y necesidades.

Llegados a este punto es vital que se ofrezca información más al detalle sobre las vulnerabilidades, entrando más en profundidad en la explotación y opciones de mitigación del ataque, así como en los parches propuestos (que componentes serán actualizados, que dependencias crea dicha actualización, si se introducen modificaciones adicionales, etc.).

Bienvenida sería la opción de desactivar todas las dependencias y conexiones externas y automáticas, tanto a nivel de servidores como de estaciones de trabajo. Así como documentar el proceso de WindowsUpdate y facilitar su personalización, posibilitando a los administradores establecer sus propias políticas y sistemas internos de autoactualización según necesidades. Aunque Microsoft ya dispone de soluciones propietarias para la distribución de parches, su adopción sólo optimiza recursos y cambia el problema de sitio, pero no permite corregir la situación de dependencia y falta de control.

Bernardo Quintero

Entrevista



Hector Montenegro

Hector Montenegro fue responsable de seguridad de Microsoft en España en los tiempos duros, desde el 2001 al 2003, sabe como nadie qué es enfrentarse a las críticas (fundadas) sobre seguridad en productos de Microsoft y tener poco con lo que "defenderse".

Hispasec: ¿Cuál y cómo fue tu primer contacto con Hispasec?

Hector Montenegro: Mi primer contacto "personal" con Hispasec lo recuerdo perfectamente. Fue en diciembre del año 2001. Año especialmente activo en términos de "incidencias" masivas de seguridad. Lanzamos un programa de Protección tecnológica (STPP) y necesitábamos credibilidad, consejo, opinión experta, etc.

H: ¿Estás suscrito a una-al-día? ¿desde cuándo?

HM: Sí, estoy suscrito desde el año 1998. Recuerdo que en aquel entonces era el responsable de Seguridad de la empresa DINSA.

H: ¿Cómo influyó una-al-día e Hispasec en el departamento de seguridad de Microsoft (si es que lo hizo)?

HM: Sí que lo hizo, desde varias perspectivas. La primera, porque la noticia de una-al-día era de

lectura obligatoria y diaria. Si en algún momento aparecía una noticia relacionada con Microsoft, sabía perfectamente que ese iba a ser motivo de conversación con la visita, cliente, partner que tuviera ese día. ¡Teníais mucha influencia!

Y por otro lado, Hispasec tuvo la generosidad en su momento de "ilustrarnos" y abrirnos los ojos sobre muchos aspectos de la seguridad real que nos podían pasar desapercibidos. De forma amigable, pero rotunda. Tuvisteis mucha mas influencia de lo que pensáis llevándonos a una fuerte autocrítica. Indispensable para mejorar.

H: ¿Cómo y por qué te metiste en esto?

HM: Cuando comencé a trastear en el año 1994 con un disquete promocional de Compuserve adjunto a no sé qué, quién me iba a decir entonces que eso iba a modificar de alguna forma la prometedora y meteórica carrera que como Físico había emprendido hacia el Nobel ;-) desde una empresa de I+D del entonces Instituto Nacional de Industria, enfrascado en publicar el máximo número de artículos posible sobre Simulación Computacional. Sin apenas darme cuenta, me vi sustituyendo mis libros de "Computational fluid Dynamics" o "Coal combustión simulation" por "Los secretos de la Seguridad en Internet", "Programación en Internet" o "Net Privacy".

H: ¿Piensas que se ha perdido el "romanticismo" de aquellos primeros días en la red?

HM: ¿Romanticismo? Respondo a nivel personal, y recordando el 1995 entre las cuatro paredes de mi habitación. Éramos era una pandilla de "taraos" a los ojos de muchos. Hablando de dominios, proveedores, seguridad... ¿Seguridad? ¿Pero de qué me está hablando este buen hombre que no se levanta del ordenador? Lo recuerdo como un campo de experimentación constante. Como un campo de pruebas y de permanente sorpresa. Para mí era tal la pasión que sentía cada vez que descubría algo nuevo, que la red terminó en convertirse en un auténtico devorador de tiempo, y finalmente en una parte importante de mi futura profesión (reconoceré haber dejado en el camino una expulsión de mi ISP, y es que trastear con la seguridad nunca fue del agrado de todos ;-))

H: Si bien es cierto que a partir del 2002 el propio Bill Gates centró atención y recursos en mejorar todos los aspectos de seguridad, Microsoft aún mantiene una imagen cuando menos cuestionada en este área. ¿Cuánto hay de herencia del pasado y cuánto de realidad en las críticas actuales? ¿A día de hoy es un problema más de imagen que de tecnología?

HM: Absolutamente. Es evidente para los profesionales de la seguridad el gran esfuerzo que se ha hecho y se sigue haciendo desde Microsoft, en todas y cada una de las fases relacionadas con la seguridad de un producto. Muchas de las acciones criticadas ferozmente por muchos (actualización periódica), hoy en día son imitadas por casi la totalidad de fabricantes.

Todos sabemos que la seguridad es un arduo proceso. En una ocasión vi la seguridad definida como "un estado de ánimo". Pero no cabe duda que con frecuencia nos encontramos con una inercia (interesada y alimentada por competidores) a modificar prejuicios relacionados con la seguridad en Microsoft y perpetuar una imagen que no corresponde con la realidad actual. Y pondría muchos ejemplos como los relacionados con ORACLE o Apache en su comparación con SQL Server o IIS respectivamente. Los problemas de seguridad de los primeros suman más de 10 veces los problemas de seguridad de los segundos, y sin embargo la percepción no va en consonancia con este dato.

H: Suponemos que a lo largo de los años te habrás encontrado en más de una situación

“hostil” a la hora de dar conferencias como responsable de seguridad de Microsoft, por ser objeto de crítica tanto por parte de ponentes (nosotros hemos participado en alguno) como de público. ¿Has observado alguna evolución en las críticas durante estos años o son recurrentes?

HM: Sí, en efecto ser responsable de seguridad de Microsoft en los tiempos “heavies” del 2001 al 2003 fue una experiencia y un sobresalto. Recuerdo especialmente aquella ocasión (2001) que vosotros también recordáis en el evento e-Gallaecia, en el que permanecí durante tres días completos, sentado en primera fila, escuchando las “dedicatorias” de bastantes ponentes, y tomando notas como un descosido para responderles adecuadamente en mi intervención posterior. Afortunadamente mi intervención era la última del último día (había morbo, y por eso me dejaron hasta el final ;-) , pero el número de alusiones en tres días había sido tan enorme, que responder a todas ellas fue un reto. Recuerdo especialmente la mención que os hice en aquel evento (estabais entre el público) a sabiendas de que vuestro sitio web se encontraba sobre Windows NT, sin protecciones perimetrales, configurado con conocimiento y criterio de forma que nunca había sufrido un percance de seguridad a pesar del elevado número de ataques. Asíque me servisteis de ejemplo para hablar de la “vulnerabilidad de capa 7” ;-) .

La hostilidad hacia Microsoft en debates públicos acerca de la seguridad, no tiene nada que ver en la actualidad. Especialmente gracias a que lo que en el 2001 eran solo promesas, con el tiempo se iban plasmando en realidades y argumentos con los que te sentías mas “protegido” (es decir, common Criteria, Secure Development lifecicle, reducción del 60% en número de vulnerabilidades, etc.). En el 2001 me sentía como si Microsoft me daba una navajita cortaúñas y me decía: “Ale chaval, haz lo que puedas”. Ahora sinceramente siento que la “navajita cortaúñas” es un bazuca. Recuerdo también de forma especial la mesa redonda en Securmatica sobre la seguridad en código abierto vs. propietario. Toda una experiencia ;-)

De estas he tenido unas cuantas, pero reconozco que la mayor “pasión” en debates estaba aún por llegar. Y es que el “apasionamiento” cuasi religioso que traen consigo los temas relacionados con la competencia Open Source vs. software propietario, hacen que ese tipo de experiencias sobre seguridad las recuerde casi como un juego de niños. Lo “mejor” estaba aún por llegar (frase un tanto masoquista, lo sé).

H: En una industria tan bien asentada y especializada como la de los antivirus, ¿qué impulsó a Microsoft a entrar de lleno con sus propias soluciones? ¿Simplemente negocio o sintió la necesidad de mejorar en algún aspecto que no era cubierto por las compañías antivirus?

HM: No fue un aspecto relacionado con “falta de confianza”. Es más, los grandes fabricantes antivirus son muy buenos socios de Microsoft con un enorme conocimiento y experiencia. Pero sí veíamos importante el aumentar nuestro conocimiento sobre el mundo de la seguridad (no solo desde la perspectiva de desarrollo seguro de código y de respuesta a emergencias) y participar de la evolución de ese mercado. Tenemos más capacidad de entender los problemas de seguridad, reaccionar de forma más sólida y colaborar más eficazmente con nuestros socios de seguridad ahora que antes.

H: ¿Cuál es el sitio más interesante en el que has estado por trabajo?

HM: Desde la perspectiva lúdico-festiva, sin duda el viaje que aproveché para visitar unos días el parque natural de Banff en plenas montañas Rocosas en Canada. Una vez pasada la aprensión a ser devorado por un oso, los paisajes de los que ahí se disfrutan son “indescriptibles”, además de circular por la alucinante Autopista de Hielo que recorre el parque, dicen que la más espectacular de América, y no es para menos.

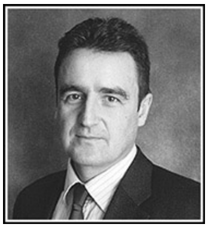
Prohibido tocar el freno, por razones obvias. Desde la perspectiva profesional, pues es difícil. Quizá, y por ser mas reciente, la reunión en San Francisco que describo en este post http://blogs.technet.com/hectormontenegro/archive/2008/05/26/alucinante-reuni-n.aspx (sí, sin duda, estoy aprovechando para hacer publicidad de mi blog ;-))

H: ¿Por dónde andarán los tiros en seguridad en el futuro?

HM: Esto siempre es una aventura, pero a nivel de investigación básica creo que los avances en criptografía cuántica marcarán el futuro de la seguridad en función de su capacidad de implementación de bajo coste y accesibilidad.

H: ¿A qué dedicas más tiempo últimamente?

HM: Esa pregunta me hace sospechar que no tienes hijos, ¿Verdad? Pues el tiempo no profesional a mi familia, a la música (aporrear baterías y guitarras me vine relajando desde los 18 años), a la lectura (recomiendo Un dia de Cólera. Alucinante) y a la montaña. Si la pregunta iba más por el lado profesional, te reconoceré que hace un par de años no me dedico con la misma intensidad a la seguridad, y si por el contrario al mundo de los estándares (OpenXML,) interoperabilidad, a pelearme en mi blog (http://www.hectormontenegro.com), aunque no perder la seguridad de vista sigue siendo una satisfacción.



7D3

3723

1111010011

Capítulo 5

AÑO 2003



1041379200 – 1073001599



Durante este año...

_ El 23 de enero se recibe la última señal del mítico **Pioneer 10**, una aeronave espacial lanzada al espacio en 1972 que hizo las primeras observaciones de Júpiter. Se perdió su señal cuando estaba a unos 12.000 millones de kilómetros de la Tierra.

_ El 14 de febrero muere la **Oveja Dolly**. Fue el primer mamífero clonado en 1996. Su muerte se debe, entre otras posibles causas, a la antigüedad genética del núcleo de la célula adulta que le fue transferida. Aunque cuenta cronológicamente con más de 5 años, ya tiene artritis. Genéticamente suma 11 (hay que sumar los 6 de la edad genética de la madre).

_ Vodafone sufre una avería el 20 de febrero que deja **sin teléfono** móvil a sus casi 9 millones de abonados en España.

_ Aparece **Second Life**, un mundo virtual desarrollado por Linden Research Inc. Obtendría una atención y popularidad cada vez mayores a partir del año 2006, cuando las empresas comienzan a montar sus sedes virtuales dentro de este lugar que parece atrapar a sus participantes. Gaspar Llamazares, coordinador de Izquierda Unida tiene su propio personaje de Second Life y la delegación del PP en Castilla La Mancha cuenta con una oficina electoral. Se montarían, incluso, manifestaciones virtuales contra las sedes de partidos políticos. Se crea toda una jerarquía y mundo paralelo, que se refleja en cifras muy reales al vender en la vida real las cuentas de personajes poderosos en Second Life. A finales de 2004 se lanzaría World of Warcraft, otro mundo virtual con mucho éxito.

La **guerra contra Iraq** comienza a materializarse. Los líderes del Reino Unido, España, Dinamarca, Hungría, Italia, Polonia, República Checa, Portugal y Rumanía demuestran su apoyo a los planes de Estados Unidos para invadir el país. Francia muestra su rechazo y Estados Unidos cambia el nombre de sus "French Fries" (con este nombre se conocen allí las patatas fritas) por "Freedom Fries".

El 15 de febrero 10 millones de personas en más de 600 ciudades de todo el mundo se manifiestan en contra de la guerra. Al día siguiente, todos los grupos de oposición del Parlamento español apoyan una moción contra la posición de Bush y Aznar. El 16 de marzo, Aznar, Blair y Bush se reúnen en la conocida "foto de las Azores" donde los tres argumentan que, según palabras del propio Bush, "es el momento de la verdad". Se da un ultimátum de 48 horas a Iraq para forzar el desarme inmediato. Bush insiste en que la operación será corta y eficaz.

El desarme no se produce y el día 19 de marzo, las primeras bombas caen sobre Baghdad. Ni Saddam Hussein ni sus hijos abandonan el país. Los hijos de Hussein morirían el día 22 de julio en manos de las tropas de los Estados Unidos. El 9 de abril las fuerzas estadounidenses conquistan la capital Baghdad, y para el 1 de mayo, George W. Bush anuncia a bombo y platillo que la misión se ha conseguido y que los combates se dan por concluidos en el país.

En marzo de 2008 se llegaría a los 4.000 militares estadounidenses muertos en la guerra. Los civiles y militares iraquíes muertos se cuentan por decenas de miles bajo una atmósfera de continuo miedo y ataques terroristas en las principales ciudades del país.

_ El 14 de abril se completa el **genoma humano** con un 99.99% de precisión. Concluye así la carrera hacia el conocimiento de la genética humana.

_ El 26 de mayo de 2003, un avión**Yakovlev 42-D** de fabricación rusa se estrella en Turquía cerca del aeropuerto de Trebisonda con 75 personas a bordo. Entre ellos, 62 militares españoles que regresaban a España después de cuatro meses de misión en Afganistán y Kirguizistán. Mueren todos junto a 12 tripulantes ucranianos y un ciudadano de origen bielorruso. El accidente se convierte en la peor tragedia del Ejército español en toda su historia en tiempo de paz.

_ Durante el verano, se vive una **ola de calor** en todo el mundo. En el Reino Unido se alcanzan los 38,5 grados centígrados en agosto. Paris llega a los 44.

_ En la una-al-día del 23 de agosto "Nuevo caso de **"phishing"**, esta vez con Citibank" se incluye por primera vez el término phishing. Hasta ahora se venía usando la expresión genérica "fraude online".

_ A principios de octubre **Arnold Schwarzenegger** es elegido como gobernador de California, abandonando su carrera de actor.

_ El 20 de noviembre **Michael Jackson** es arrestado con cargos de abuso infantil.

_ El día de Nochebuena la policía española frustra un ataque de **ETA**. Pretendía colocar 50 kilos de explosivos en la estación de Chamartín de Madrid.



_ El 26 de noviembre el **Concorde** realiza su último vuelo. El primero lo realizó en 1969, comenzando el servicio comercial en 1976. Se convirtió en un icono de la aviación durante los 80 y 90, muy popular debido a su diseño futurista y velocidad supersónica. El vuelo Air France 4590 realizado por un Concorde de París a Nueva York, se estrelló en Francia el 25 de julio de 2000 con 109 personas en su interior. Todas murieron. El incidente se produjo por una pieza de titanio que se había desprendido de un despegue anterior en la misma pista desde donde salía el Concorde. Aunque se consideraba el avión más seguro del mundo, con respecto al ratio pasajeros fallecidos y distancia viajada, este accidente marcaría el principio del fin del Concorde. La crisis económica tras los atentados del 11 de septiembre, junto con otros factores, pusieron punto y final a sus vuelos a finales de 2003.

_ Se crea el **Proyecto Fedora**. La mítica Red Hat Linux es descontinuada y se recicla en forma de Red Hat Enterprise Linux (RHEL). Se trata de la distribución de Linux oficialmente soportada por Red Hat, orientada a empresas. Fedora se convertiría en un proyecto comunitario como lo había venido siendo hasta ahora Red Hat Linux. Red Hat Linux 9 dejaría de ser soportada oficialmente en abril de 2004, aunque el proyecto Fedora Legacy continuó publicando actualizaciones hasta finales de 2006. Fedora ganaría gran popularidad con un elevado número de versiones. La versión 1.0 de Red Hat fue presentada el 3 de noviembre de 1994.

Seguridad Informática



_ Durante el año 2003, hasta **60 millones de europeos** usan la banca online para gestionar sus ahorros, en contraste con los 23 millones que hacían uso de este servicio en el año 2000. Las bases para el **phishing** y el fraude online se asientan.

_ El mes de enero se inaugura con la detección del virus **Avril** (o Lirva, Avron o Naith). Se propaga a través del correo electrónico, unidades de redes locales, IRC, ICQ y Kazaa, además de robar contraseñas. Hace referencia a la cantante Avril Lavigne, a la que el gusano dedica el "payload". Consigue una gran difusión. En pocas horas se sitúa en segunda posición en los indicadores de infección, sólo por debajo de Klez. Pocos días después aparece **Sobag**, un gusano de gran propagación que ataca con fuerza en Estados Unidos y países anglosajones. La difusión de estos virus se realiza todavía de forma clásica, con un adjunto en un mensaje de correo... pero esto no tardaría en cambiar.

Irrumpe en escena a finales de enero **Slammer**, un gusano en el sentido más literal del término que haría historia. Aprovecha una vulnerabilidad de Microsoft SQL Server. Slammer se conecta, aprovecha el fallo y ejecuta un pequeño código que busca nuevos servidores a los que infectar. En apenas unos minutos los servidores infectados se elevan exponencialmente, hasta que la Red completa sufre una pequeña saturación. Cada 8,5 segundos se dobla el número de sistemas infectados y en sólo diez minutos consigue introducirse e infectar a 75.000 ordenadores. Se cuela en la red de monitorización de una central nuclear, dejándola inoperativa durante cinco largas horas. Slammer no se escribe como archivo, sólo existe en la memoria de los sistemas infectados, lo que complica la detección por parte de los antivirus.

El gusano actúa enviando un paquete UDP de 376 bytes al puerto 1434, y aprovecha una vulnerabilidad de desbordamiento de memoria intermedia existente en este servicio para forzar la ejecución automática del código. El puerto 1434 es usado por los clientes para consultar cuál es el puerto TCP asignado a un servidor SQL virtual en particular. La vulnerabilidad fue documentada por Microsoft el 24 de julio de 2002, fecha desde la que está disponible un parche específico para corregirla.

_ En agosto el gusano **Sobig** bate un récord: Messagelabs lo califica como el virus con la propagación más rápida de la historia.

_ En febrero The Washington Post publica que el presidente de los Estados Unidos ha firmado una directiva secreta en la que ordena al gobierno desarrollar, por primera vez, un plan nacional que fijará cuándo y cómo **lanzar ciber-ataques contra las redes informáticas del "enemigo"**. El Pentágono prepara los planes para establecer todos los pasos necesarios para desarrollar una actuación hostil contra la infraestructura informática de un país enemigo. Se compara esta directiva con la existente para el uso del armamento nuclear, que establece las situaciones en las que puede utilizarse este tipo de fuerza, la selección de objetivos que se consideren legítimos y quién debe autorizar un ataque de este tipo. El periódico norteamericano indica que todo el desarrollo se ha realizado internamente por organismos públicos (Pentágono, CIA, FBI y NSA). Un mes antes se había solicitado por primera vez la opinión de

expertos externos, en una reunión celebrada en el MIT. De acuerdo con la noticia, diversos investigadores expresaron sus reservas en participar en este tipo de planes bélicos.

_ **VISA y MasterCard** reconocen que los datos de más de **cinco millones de tarjetas de crédito** se han visto comprometidos. Algunas fuentes elevan la cifra hasta los 8 millones, al incluir las tarjetas de American Express, también afectada. El atacante obtuvo los datos de los números de tarjetas de crédito tras comprometer la seguridad de una tercera compañía encargada de procesar las transacciones de las tarjetas de crédito en nombre de comerciantes.

_ Se detecta a finales de febrero **Lovgate**, cuya peculiaridad es que responde a los correos reales. Entre otras técnicas, el gusano se distribuye por email simulando ser respuestas a los mensajes nuevos que se encuentran en la bandeja de entrada de los usuarios infectados. Esta simple técnica de ingeniería social (que contrasta con los asuntos fijos usados en general por el malware hasta la fecha) le hace escalar puestos rápidamente como gusano de gran propagación.

_ Se popularizan nuevos métodos de envío de spam usando el **servicio Messenger** de Windows. El servicio Messenger (no confundir con el Microsoft Messenger o el MSN Messenger ni con ningún programa de navegación web o lectura de correo electrónico) es un servicio de los sistemas operativos de la familia Windows que implementa un sencillo sistema de envío de mensajes y avisos entre las máquinas conectadas en la red local. Los mensajes emergentes utilizan el protocolo NetBIOS, por lo que cuando circulan por una red TCP/IP utilizan los puertos 137 (UDP) y 139 (TCP). Este es el mecanismo habitual de transmisión para los mensajes enviados mediante un NET SEND o la API NetMessageBufferSend. Los mensajes se presentan en una ventana de Windows, con el título “Mensajería de Windows”, con el texto del mensaje y un botón “Aceptar”. Al pulsar el botón, la ventana se cierra. La mayoría de los usuarios no se protegen detrás de ningún cortafuegos en ese momento, y se encuentran con que, cada cierto tiempo, desde Internet se le envía a través de este molesto sistema (que obliga a aceptar o cerrar una ventana emergente) anuncios sobre viagra y otros productos. Incluso se anuncian de esta forma programas fraudulentos que prometen evitar este tipo de spam en el sistema (simples ejecutables que detenían el servicio en Windows). Con el Service Pack 2 para Windows XP, Microsoft deshabilitaría por defecto el servicio “Mensajero” o “Messenger”.

_ En marzo **Sendmail** vuelve a sufrir una grave vulnerabilidad. Las versiones anteriores a la 8.12.8 son susceptibles a un ataque que permite que un usuario remoto ejecute código arbitrario en el servidor de correo, con privilegios de administrador.

_ El estudio **“Decimalisation table attacks for PIN cracking”** demuestra la vulnerabilidad de los sistemas de seguridad utilizados por los cajeros automáticos para la validación de los PIN asociados a las tarjetas de crédito. Dos investigadores de la universidad de Cambridge (Reino Unido) presentan un estudio de las debilidades existentes en los dispositivos hardware para el almacenamiento seguro y la validación de los PIN asociados a las tarjetas de crédito utilizadas habitualmente por las instituciones financieras. Citibank intenta ocultar la información, que finalmente sale a la luz.

_ Marzo de 2003 es un mes especialmente prolífico en cuestión de vulnerabilidades. En apenas dos semanas, se publican **graves vulnerabilidades** para Sendmail, BIND, Flash, Snort, Internet Explorer, WebDAV, Windows Script Engine, Samba y el kernel de Linux.

_ Se descubre la vulnerabilidad en el servicio RCP Endpoint Mapper presente por defecto en el puerto TCP/135 en Windows NT 4.0, 2000 y XP. Microsoft publica el parche para Windows 2000 y XP, mientras

que deja a todos los sistemas Windows NT vulnerables, con la única excusa de que la solución en este sistema es muy complicada. **Es el principio del fin para NT**.

_ En marzo se descubre una debilidad en el **protocolo de autenticación NTLM**. Todas las versiones de Windows utilizan el protocolo SMB para los servicios de compartición de archivos e impresoras. Cuando un cliente se conecta a un recurso de la red, se utiliza la autenticación NTLM para enviar las credenciales de usuario incluyendo la contraseña. Un servidor SMB especialmente manipulado puede utilizar esta información para autenticarse en el cliente, llegando a poder obtener pleno control sobre los recursos compartidos en el cliente.

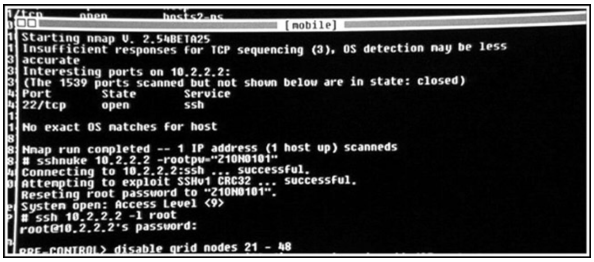
_ Es el año de los problemas en los servidores web más populares. **Netcraft** supone el mayor repositorio de información sobre estadísticas de servidores web. En la encuesta de marzo se basa en las respuestas de casi cuarenta millones de servidores, en la que se refleja la posición dominante de Apache con un 63% del mercado. La Fundación Apache lanza la voz de alarma sobre un grave riesgo de denegación de servicio en las versiones que van de la 2.0 a la 2.0.44 de su servidor web. Los detalles de la vulnerabilidad no se conocerían hasta el ocho de abril, pero el grupo advierte a los usuarios antes de que se hagan públicos estos detalles. Este comportamiento les viene a redimir ante una embarazosa situación que sufrió la Fundación en junio de 2002, cuando los detalles de su peor problema de seguridad conocido hasta la fecha fueron públicos antes de que ellos mismos tuvieran la solución y pusieran a disposición de los usuarios el parche adecuado. IIS sufre de un problema de ejecución de código a través de WebDAV también por esas fechas. Un estudio de Netcraft afirma que tres cuartos de los sitios web que operan con este IIS 5.0 lo hacen con el protocolo WebDAV habilitado y por lo tanto son vulnerables al fallo.

_ **Alan Ralsky**, el rey del spam, recibe un auténtico ataque distribuido de denegación de servicio. Se inunda de basura su correo físico postal. En 2003 Alan Ralsky es uno de los personajes más prolíficos en el envío de correo basura a través de Internet, con una larga trayectoria iniciada en 1997. En diciembre de 2002 Ralsky concedió una entrevista donde ridiculizaba y se reía de toda la comunidad contraria a la existencia del spam y que valora la intimidad de su buzón de correo. Se quejaba, por ejemplo, del coste que le suponía tener toda su infraestructura en China ante la imposibilidad de utilizar las empresas norteamericanas. En esa entrevista cometió el error de comentar que su casa estaba situada en una población del estado norteamericano de Michigan. Esta entrevista es reproducida en slashdot.org y uno de los lectores encuentra la dirección postal del domicilio del spammer. De forma totalmente espontánea, otros lectores utilizan esta dirección para suscribir al spammer a catálogos comerciales, revistas de anuncios, panfletos, solicitudes para recibir información, etc... Otros van más allá y le envían directamente basura (en el sentido literal de la palabra).

_ En mayo **Fyodor**, el autor del popular "Nmap", publica los resultados de una encuesta realizada entre sus usuarios, detallando las herramientas de seguridad más utilizadas.

_ Todos los medios especializados se sorprenden de una escena inusualmente realista en la popular película **The Matrix Reloaded**. Transcurridos aproximadamente dos tercios de la película, Trinity se sienta delante del ordenador. En este punto, en lugar de aparecer las típicas pantallas de "acceso denegado" o "introduzca la contraseña" de aspecto irreal, Trinity utiliza Nmap, una potente herramienta para determinar qué servicios ofrece una máquina conectada en Internet. La escena es muy breve, unos pocos segundos, pero suficientes para reconstruirlos. Trinity, desde una sesión root en una máquina Unix (identificable por el prompt #), utiliza Nmap 2.54BETA25 para identificar los servicios que ofrece la máquina 10.2.2.2. Encuentra el puerto 22 (TCP), correctamente identificado como SSH. A continuación, utiliza un programa llamado sshnuke que muestra este texto "Attempting to exploit SSHv1 CRC32". Se trata de un exploit que le permite cambiar la contraseña del usuario root del sistema remoto. Si bien no se

tiene constancia de la existencia de ningún exploit llamado “sshnuke”, lo que sí es real es la vulnerabilidad y también sus efectos. Otro aspecto interesante es la ubicación temporal. La versión de Nmap utilizada fue publicada el 4 de junio de 2001 y la vulnerabilidad que explota el sshnuke, el 8 de febrero de 2001. En la primera película “The Matrix”, la acción se sitúa temporalmente en 1999. Morpheus indica, en la nueva película que “durante estos seis meses” (desde el momento en que Neo se transforma en “The One”) “se han liberado más mentes que en los seis años anteriores”. Por tanto, la acción de “The Matrix Reloaded” transcurre en un mundo simulado en los alrededores del mes de junio de 2000. Trinity utiliza una vulnerabilidad y una versión de un producto todavía no publicados.



En junio se descubre un gusano que simula ser un **test enviado desde Hispasec**. El archivo que se adjunta en el correo es en realidad un nuevo gusano que está siendo distribuido desde Hotmail. El mensaje tiene el siguiente aspecto:

Remite: “test@hispasec.com”
Asunto: “Tests antivirus para comprobar la protección del e-mail”
Adjunto: “eicax.com”

Cuerpo: “Hispasec pone a disposición de todos los usuarios dos tests para comprobar el correcto funcionamiento de la protección antivirus del correo electrónico. El primero de ellos nos indicará la correcta instalación y buen funcionamiento del antivirus, mientras que el segundo determinará la capacidad de detección proactiva para identificar gusanos que explotan vulnerabilidades conocidas.”

El adjunto tiene un tamaño de 180.736 bytes, resultado de comprimir con UPX el ejecutable original de 438.784 bytes, al parecer escrito en Delphi. En el código se puede apreciar como, además del mensaje simulando un envío de Hispasec, se encuentran otros muchos textos para construir otros e-mails y utilizarlos como anzuelo. Entre otras temáticas, hacen referencia a Hotmail, Microsoft, Madonna, Spam, SARS, otros sitios de información sobre virus y seguridad (además de Hispasec), chistes, etc., todos en español.

Consigue cierta repercusión en los países de habla Hispana. Obviamente se trata de un mensaje falso que utiliza la imagen de Hispasec como reclamo.

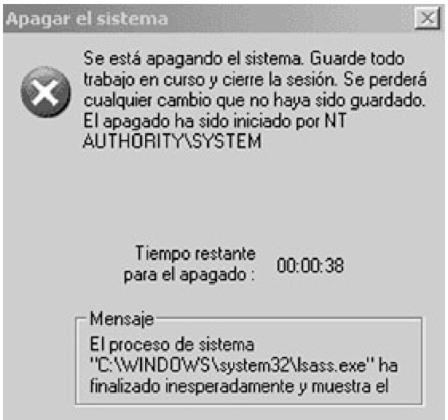
_ Se comienza a observar, de forma generalizada, la **alianza entre spammers y troyanos**. El spam se multiplica, tomando dimensiones de plaga (y todavía tendría que crecer mucho más). Se comienza a dudar de la eficacia de los métodos habituales y poco efectivos que se vienen utilizando en contra del correo basura hasta la fecha. Las protecciones habituales son poco eficaces e incluso ingenuas ante un problema creciente. Se comienza a detectar cada vez más el uso de de troyanos que tienen como fin el envío de spam desde los sistemas infectados. Al realizarse el envío de forma distribuida entre múltiples sistemas es mucho más complicado identificar todos los puntos de envío para introducirlos en las listas negras.

_ En junio Microsoft publica el **Service Pack 4** para Windows 2000, que sería el último.

_ En julio, desde una página web asociada a **Zone-H** (la web de los "defacers") se propone un concurso. Ganan aquellos que primero consigan atacar y modificar 6.000 sitios web en 6 horas o, en su defecto, el que logre la cifra más alta en ese plazo de tiempo. El domingo 6 de julio, día del concurso, se espera una avalancha de páginas desfiguradas, los medios tradicionales se encargan de exagerar la jugada. La repercusión sería escasa o nula, entre otras razones por un supuesto ataque de denegación de servicio a la propia Zone-H. La organización, participación, y objetivos del concurso resultarían todo un fiasco.

_ Aparece en julio **Migmaf**, un troyano que convierte los PCs en servidores de páginas pornográficas. Destaca por instalar un proxy reverso en el ordenador infectado que redirecciona las peticiones HTTP contra un servidor central, habitualmente con contenido pornográfico. De esta forma, se consigue ocultar la ubicación real de ese servidor central, impidiendo cualquier posible acción de bloqueo de su contenido.

_ En julio se descubre el desbordamiento de memoria intermedia en la interfaz RPC de sistemas Windows que, a la postre, permitiría la aparición del fatídico gusano Blaster. **Remote Procedure Call (RPC)** es un protocolo usado para proporcionar mecanismos de comunicación entre procesos de forma que un programa que se ejecute en un sistema pueda ejecutar código en otro sistema remoto de forma transparente. La implementación de Microsoft de este protocolo está derivada del protocolo RPC de la OSF (Open Software Foundation) pero con la inclusión de algunas extensiones específicas de Microsoft. En el caso de Windows, el servicio RPC está asociado al puerto 135 (TCP). El fallo se localiza en la parte de RPC que negocia con el intercambio de mensajes sobre TCP/IP. Lo provoca por un tratamiento incorrecto de mensajes mal construidos. Para explotar esta vulnerabilidad, un atacante debe enviar peticiones especialmente manipuladas al sistema remoto a través del puerto 135.



En agosto saltan todas las alarmas. Se comienzan a recibir informes de un nuevo gusano que utiliza la reciente vulnerabilidad descubierta en el mecanismo RPC de todas las versiones de Windows. **Blaster** oscurece el verano de 2003. Uno de los efectos de este gusano es que provoca el reinicio del ordenador infectado cada pocos minutos. El gusano realiza un barrido de las direcciones IP con el objeto de identificar los sistemas Windows vulnerables (sistemas con el puerto 135 accesible). Cuando detecta la existencia de un sistema vulnerable, utiliza la vulnerabilidad RPC para abrir una sesión de la consola (cmd) accesible de forma remota a través del puerto 4444. Ataca a los ordenadores que utilizan cualquier versión de Windows del momento. Para cada dirección IP obtenida, el gusano analiza las 20 direcciones IP siguientes, intentando establecer una conexión en el puerto 135. Si la conexión es satisfactoria, el gusano utiliza dos exploits diferentes para intentar infiltrarse en el sistema remoto. El primero de estos exploits sólo funciona si el sistema remoto ejecuta Windows 2000 mientras que el segundo es válido en el caso de que el sistema remoto utilice Windows XP. Debido a que el gusano no intenta determinar que versión de Windows utiliza el sistema remoto, sino que lanza uno u otro exploit de forma aleatoria, en el momento de enviar el código del exploit puede provocar la detención inesperada del proceso SVCHOST.EXE en el sistema atacado, lo que provocará que el sistema se vuelva inestable. En estos casos, la infección no se concluye, pero el sistema atacado puede quedar inoperativo y necesitar un reinicio. Si funciona correctamente, se abrirá una sesión

del intérprete de órdenes de Windows, asociada al puerto 4444. Dentro de esta sesión, el gusano utiliza la utilidad TFTP para transferir el código del gusano al ordenador recién atacado. Blaster se convierte en una verdadera pesadilla para millones de usuarios que ven cómo su ordenador comienza a reiniciarse cada vez que se conecta a Internet. La plaga cobra dimensiones desproporcionadas.

_ El **phishing** sigue popularizándose. Se detectan en verano fraudes contra PayPal, BBVA... Todavía no se califica específicamente de "phishing". Se usan las palabras "fraude online".

_ **Sobig.F** se propaga masivamente de forma tradicional, enviándose como adjunto en un e-mail, y a través de los recursos compartidos de las redes locales.

En agosto se anuncia que **los documentos de Word esconden información sensible.** El archivo creado con Word oculta en realidad más datos de los que pueden verse a primera vista: versiones anteriores del documento, rectificaciones o los nombres de personas que han trabajado en él, pueden quedar escondidos en el documento y extraerse posteriormente. El gobierno británico abandona el uso de Microsoft Word, en favor del formato PDF tras verse forzado a comparecer en la Cámara de los Comunes Alastair Campbell, director de comunicación y mano derecha de Tony Blair, para dar más datos de cuatro empleados cuyos nombres aparecían ocultos como autores del informe ya conocido como "dodgy dossier". Este expediente fue publicado en febrero de 2003 como fruto del trabajo de la inteligencia británica donde se evidenciaba la existencia en Iraq de armas de destrucción masiva. Poco tiempo después se demostró que el informe era en realidad un plagio que contenía copias literales de una antigua tesis de un estudiante californiano de apenas 13 años de edad.

Aunque fuese el más sonado, no se trataba de un caso aislado. Un estudio llevado a cabo en abril por Simon Byers, del laboratorio de investigación de AT&T en los EE.UU evidencia que gran parte de los documentos Microsoft Word publicados en Internet contienen información sensible oculta. Desde nombres, direcciones de e-mail, nombres de documentos relacionados, números de la seguridad social, trayectorias de las unidades y carpetas donde estaba almacenado el documento, etc. La metodología de Byers consistió en recolectar 100.000 documentos Word desde Internet de forma aleatoria. Más de la mitad de los documentos mantenían entre 10 y 50 palabras ocultas, un tercio de los mismos entre 50 y 500, y el 10% escondían más de 500 palabras en su interior.

_ En septiembre se encuentra una **vulnerabilidad crítica en Internet Explorer** que permite la ejecución de código con sólo visitar una página web. El parche acumulativo de agosto no soluciona por completo un agujero crítico que permite ejecutar código arbitrario en los sistemas con Internet Explorer. Hispasec proporciona algunas demostraciones reales de cómo la vulnerabilidad sigue existiendo, aun teniendo instaladas todas las actualizaciones disponibles hasta la fecha. El exploit elegido por Hispasec para demostrar el fallo pone del revés la pantalla. Un mes después, Microsoft soluciona el problema.

_ Aparece **Swen**, un malware que se hace pasar por una actualización de Microsoft. Envía un elaborado mensaje donde simula un envío de Microsoft con un adjunto que pretende ser una actualización. Logra engañar a muchos usuarios.

El 15 de septiembre, **Verisign** realiza una serie de modificaciones en la definición de los dominios de primer nivel .COM y .NET sin previo aviso. Se denominaría **"Site Finder"**. Estos cambios consistieron en añadir una entrada comodín para que cualquier petición de resolución de un nombre de dominio erróneo fuera automáticamente redirigida hacia un sistema (sitefinder.verisign.com), donde hay un servicio de búsqueda y directorio de páginas web. Las implicaciones de esta modificación realizada son más graves de las descritas por la compañía y afectan en gran medida al funcionamiento de la red. El cambio efectuado por Verisign puede calificarse como la modificación más importante realizada en la arquitectura del servicio de resolución de nombres desde la introducción del DNS.

La existencia de los comodines implica que cualquier petición de resolución de nombres de un dominio .COM o .NET siempre resultará satisfactoria, con independencia de la existencia real de ese dominio. Si el dominio está registrado, el cambio efectuado por Verisign no afecta en absoluto a la resolución. Continuará siendo delegada en los servidores de nombres asociados al dominio. La comunidad no tarda en responder. Además de las iniciativas para pedir la inmediata suspensión del servicio, se plantea el desarrollo de sistemas para la circunvalación de los comodines en los dominios de primer nivel. El ISC (Internet Software Consortium), que desarrolla el servidor de nombres BIND anuncia que en breve facilitará un parche para inhabilitar el cambio efectuado por Verisign. Finalmente, tras muchas protestas, el rechazo de la comunidad y varias grandes empresas, la intervención de ICANN y las demostraciones de que una modificación así supone un ultraje para los internautas, pocas semanas después el servicio se retira. Verisign insistiría poco después, sin finalmente llevarlo a cabo, en relanzarlo.



_ En octubre **Valve**, compañía desarrolladora de Half Life y "Counter Strike", "Team Fortress" o "Day of Defeat" confirma la noticia: el código fuente de la segunda parte de su esperado juego, aun en desarrollo, había sido robado y difundido por la red. Al parecer alguien había instalado un registrador de teclas en el equipo del fundador de la compañía.

_ En noviembre, las nuevas versiones "I" y "J" del gusano **Mimail** simulan ser un mensaje del servicio PayPal y solicitan al usuario datos sensibles sobre su tarjeta de crédito. Utiliza el formato de compresión ZIP para distribuirse, lo que le permite traspasar la mayoría de fltros perimetrales basados en extensiones potencialmente peligrosas. Se acercan tímidamente a lo que sería el malware 2.0.

_ Se destapa el intento de instalar una **puerta trasera en el kernel Linux**. Un análisis rutinario automático del código fuente de la última versión del kernel Linux (2.6-test) descubre el intento de implantar una puerta trasera en el núcleo. Permitiría a un atacante local obtener privilegios de administrador o root con la ejecución de una función aparentemente inocua y de uso normal. El fichero alterado fue "kernel/exit.c", y constaba de apenas dos líneas de código fuente. Estuvo disponible para descarga varias horas. Después del incidente se reforzaron las medidas de seguridad de acceso al código.

_ También en noviembre se conoce que cuatro máquinas del **Proyecto Debian han sido comprometidas**, aunque se insistía en que las fuentes del archivo principal no habían sufrido ningún incidente.

_ Las redes inalámbricas se popularizan. Un estudio realizado por la multinacional informática HP demuestra la **carencia de seguridad en las redes inalámbricas madrileñas** en particular y españolas en general. Los investigadores de HP realizan un recorrido por las calles con un vehículo, un ordenador portátil con tarjeta Wi-Fi, un software de detección de redes y una antena omnidireccional (actividad que se daría a conocer como wardriving). Con este método pudieron detectar cerca de 7.500 ordenadores y sistemas conectados a 518 puntos de acceso inalámbrico desprotegidos, constatando que cerca del diez por ciento eran de grandes empresas. "Creemos que no se conocen bien los riesgos de un punto de acceso mal configurado y sin seguridad", comentaban desde HP.

La noticia de una-al-día del 28 de diciembre, titulada **"Windows XP: sobrevivir al primer día"**, se convierte en una de las más visitadas de siempre, incluso en 2008 sigue teniendo cientos de visitas al día. Habla de cómo actuar ante la instalación de Windows XP en un sistema y cómo conectarlo a Internet de forma segura antes de que Blaster infectase el ordenador.

Una al día



03/02/2003 Antivirus: el efecto "zoo"

A la pregunta de "¿cuál sería el mejor antivirus?", una respuesta bastante obvia sería "el que detecte todos los virus". Afortunadamente atrás quedaron las campañas de publicidad engañosas que prometían protección 100% contra virus conocidos y desconocidos. Así que hoy día, demostrado una y otra vez que no pueden ofrecer garantías de protección proactiva contra especímenes nuevos, la respuesta podría quedar en "el que detecte más número de virus". Falso. Es más, el enfoque de "cuantos más, mejor" nos conduce de forma irreversible hacia peores productos antivirus. ¿Hora de cambiar?

En este artículo no pretendo entrar en nuevas tecnologías proactivas que podrían, sino sustituir de inmediato, al menos complementar los actuales sistemas por detección de firmas. Ya no sólo como evaluador, sino como desarrollador en Hispasec de algunas pruebas de concepto sobre nuevas tecnologías antivirus, soy consciente de que aun queda mucho camino por recorrer antes de que puedan equipararse a los sistemas actuales en cuanto a fiabilidad y facilidad. Esto no quita que existan algunas funcionalidades proactivas que no estarían de más en los actuales antivirus, y que algunas casas ya empiezan a implementar.

En definitiva, se trata de analizar el efecto negativo que, en los actuales sistemas antivirus de detección por firmas, provoca algunas prácticas que persiguen adulterar y engordar de forma artificial las estadísticas de virus reconocidos de cara a la galería.

Las colecciones "zoo"

En la mayoría de certificaciones y comparativas se suele enfrentar los productos antivirus contra varias

colecciones de muestras infectadas. El porcentaje de aciertos en las diferentes colecciones suele ser el indicador más determinante a la hora de valorar un producto.

Las colecciones pequeñas, de virus más significativos y activos, como la “InTheWild”, apenas presentan diferencias de resultados entre la mayoría de los productos y, más que un indicador comparativo, sirve como mínimo exigible.

Para marcar diferencias en las comparativas, y también como prueba de fuego en las certificaciones, se suele utilizar la llamada colección “zoo”, que básicamente consiste en un conjunto de todas las muestras infectadas que se posee.

La “zoo” comprende, además de los virus más relevantes y novedosos, toda muestra que el evaluador haya conseguido recolectar a lo largo de su carrera, desde los primeros virus que aparecieron, de los que hoy día ya no existen pruebas de infecciones reales, hasta aquellos que nunca han visto la luz ni infectado a nadie, pero que forman parte de pruebas de laboratorio o colecciones privadas.

Llegados a este punto, el usuario debe ser consciente que de los 60.000 o 70.000 virus que hoy día algunos antivirus afirman detectar, tan sólo unos cientos representan el 99% de las infecciones reales durante un año.

La necesidad de que un antivirus detecte un virus de los años 80 que hoy día no tiene posibilidades de propagación bajo Windows, o un virus que nunca ha salido a la luz y no ha infectado a nadie, puede llegar a ser discutible. Aunque las comparaciones y extrapolaciones en este campo no son buenas, es como si alguien se vacunara contra una enfermedad ya erradicada o contra un virus biológico de laboratorio, por si algún día resulta que hay un brote.

Pero la realidad es que la posibilidad, por remota que sea, existe, y el deber de un antivirus es ofrecer el mayor grado de protección posible, en especial si se trata de virus conocidos. Así que hasta el momento, nada que objetar.

Adulteraciones en las “zoo”

El problema real de las colecciones “zoo” es que no están depuradas. Es decir, existen muestras consideradas virus (o cualquier otra variante de malware, como gusanos, troyanos, etc.) que en realidad no lo son, ni presentan ningún efecto nocivo ni dañino. En definitiva, no tendrían que formar parte de la colección, ni tendrían que ser detectadas por los antivirus.

Para la confección de las propias comparativas antivirus de Hispasec, revistas especializadas, así como para análisis e informes técnicos, necesitamos contar con el mayor número de muestras posibles para realizar nuestro trabajo. Entre otras fuentes, regularmente recorremos las webs de creadores de virus y coleccionistas que permiten la descarga de muestras de forma pública a través de Internet y, por tanto, son especímenes que potencialmente podrían llegar a cualquier usuario.

Una de las tareas más tediosas para mantener la colección de muestras de Hispasec no es la recolección, sino la comprobación de las mismas. Afortunadamente a lo largo de los años hemos desarrollado varias herramientas que de forma automática nos hacen las primeras cribas y son capaces de descubrir las muestras falsas más comunes.

Sin embargo, son muchas las comparativas, incluida algunas certificaciones, que a juzgar por algunos

resultados no realizan una depuración de las colecciones. Como resultado, sus colecciones "zoo" están adulteradas con muestras que no son virus, y ello se extrapola a los indicadores que obtienen los diferentes productos antivirus.

Lo peor aun es que la mayoría de las casas antivirus, tal vez condicionadas por estas comparativas y certificaciones donde se podían ver perjudicadas, han optado por incluir en su base de datos de firmas esas falsas muestras como si fueran auténticos virus. Otra posibilidad podría ser la inversa, que las casas antivirus hubieran sido las primeras en incorporarlos como virus a sus bases de datos y que las comparativas los incluyeran a posteriori en sus colecciones al comprobar que algún antivirus las reconocían como virus. Independientemente de si fue primero el huevo o la gallina, el caso es que el circulo vicioso no hace más que aumentar.

Como dato, durante la comparativa antivirus que llevé a cabo en 1999 para PCActual e Hispasec, introducí un test inédito hasta la fecha, que consistió en enfrentar a los antivirus contra una serie de archivos representativos que habían quedado fuera de nuestra colección durante las cribas de recopilación al comprobarse que no eran virus reales. Los resultados son reveladores:
http://www.hispasec.com/comp_avs.asp?id=25

En realidad hay muchos otros tipos de muestras que suelen ser incluidas en las bases de datos de firmas antivirus y que en realidad no tienen ningún efecto dañino, desde binarios que ni siquiera pueden llegar a ejecutarse, porciones de virus que están corruptos y no pueden activarse, etc.

El efecto "zoo"

¿Cómo repercute el número de firmas que reconoce un motor antivirus en su rendimiento? Parece claro que existe una relación directa, a mayor número de firmas a chequear, mayores recursos necesitará, y la velocidad de proceso será menor, lo que perjudica al resto de procesos o aplicaciones que existan en el sistema.

El hecho de que los antivirus reconozcan virus falsos, además de la publicidad engañosa que pueda generar o la búsqueda de buenos resultados artificiales en comparativas y certificaciones de dudosa calidad, tiene un efecto negativo en el comportamiento del propio antivirus que puede penalizar el rendimiento del sistema e incluso hacer peligrar la seguridad del cliente.

La solución aunque pueda parecer sencilla, bastaría con depurar las firmas de detección de los antivirus, tiene efectos negativos inmediatos a nivel comercial: podrían verse perjudicados en comparativas y certificaciones que cuenten con muestras falsas. Es la pescadilla que se muerde la cola.

Las casas antivirus se encuentran en muchas ocasiones en la encrucijada de diseñar sus productos pensando en la protección real del usuario o en los requisitos de los evaluadores. Paradójicamente, además de no coincidir en algunas ocasiones, pueden existir incluso intereses opuestos. Normalmente se opta por un punto intermedio, intentar acometer los requerimientos de ambos, aunque a costa del detrimento en la optimización del producto.

Llegados a este punto, no debemos caer en la tentación de arrojar sobre las espaldas de las casas ntivirus toda la responsabilidad. De hecho, buena parte de esta percepción errónea de lo que debe ser un buen antivirus es achacable a las revistas especializadas y analistas que nos dedicamos a crear opinión sobre las soluciones antivirus.

Si más de una vez he dicho que muchos productos antivirus se encuentran anclados en el pasado, por no integrar nuevas tecnologías de detección más allá de las firmas, las comparativas y certificaciones están mucho peor. Uno de los casos más sonados fue el de la comparativa antivirus de CNET en 2001, entre otros despropósitos, llegaron a utilizar simuladores de virus en vez de muestras reales para algunos tests. Por lo demás, la mayoría siguen basando su modelo de evaluación en arcaicas pruebas de detección ITW y Zoo.

Soluciones

Las comparativas y certificaciones deben de evolucionar, incluyendo nuevos tests acorde con las características de las nuevos especímenes que aprovechan Internet para su propagación, así como evaluaciones que contemplen las nuevas tecnologías antivirus que se están incorporando. Por otro lado, deberían de incorporar mecanismos para la depuración de sus colecciones para evitar el efecto "zoo", incluyendo tests de detección de falsos virus cuyos indicadores se relacionen con tests de rendimiento del motor.

Los antivirus deberían de dejar de utilizar el concepto de número de virus detectados como arma de marketing, ya que no tiene ningún sentido que sigan en una guerra de cifras que de sobra saben no tiene ningún valor real y que tarde o temprano terminará por perjudicarles. Además, deberían optimizar su base de datos de firmas para reconocer sólo los especímenes que realmente pueden llevar a cabo acciones dañinas, eliminando los falsos virus. En caso de verse perjudicados en comparativas o certificaciones que utilicen colecciones "zoo" no depuradas, con muestras falsas, deberían denunciar públicamente los resultados.

Los usuarios deben de tomar conciencia de que el número total de virus que dice reconocer un antivirus es un dato sin ningún valor. Además de todo lo comentado con anterioridad respecto a los falsos virus, la propia tecnología de detección por firmas lleva a resultados dispares. Por ejemplo, dado 10 variantes de un mismo virus, un producto puede necesitar 10 firmas diferentes mientras otro puede detectar las 10 variantes de forma más genérica con sólo 2 firmas. A efectos de marketing, el primero sumará 10 virus mientras que el segundo contará sólo 2, sin embargo la detección del segundo producto es más genérica y efectiva. Tan sólo las comparativas con colecciones depuradas pueden ofrecer las diferencias reales entre el poder de detección de los distintos motores antivirus, nunca el número de virus que el propio producto anuncia.

Bernardo Quintero

28/03/2003 Antivirus: ¿especialización o navaja suiza?

Filtros de contenidos, firewalls, y ahora funcionalidades anti-spam y detector de intrusiones. Cada vez son más los antivirus que dejan de ser herramientas especializadas en la detección del malware y amplían sus funciones.

La carrera por la integración de aplicaciones de seguridad ha comenzado. Las casas antivirus están en una espiral de crecimiento a la búsqueda de poder ofrecer soluciones completas, tanto productos como servicios, que puedan abarcar todas las necesidades de seguridad de empresas y usuarios finales. En este último sector es donde aparecen en escena las suites de seguridad, partiendo del núcleo del antivirus como herramienta con mayor implantación y éxito en el mercado.

Que las amenazas de seguridad han aumentado y mutado con respecto a épocas pasadas es evidente. Hoy día la instalación de un antivirus clásico no garantiza la seguridad de un sistema, han surgido nuevas amenazas que van más allá de los virus. De igual forma, la propia evolución del malware, en estrecha relación con Internet, pone en entredicho la detección basada en firmas y requiere nuevas estrategias para detectar de forma más proactiva y genérica a los nuevos especímenes con gran poder de propagación en apenas minutos.

Llegados a este punto surgen algunas dudas, partiendo de la relativa necesidad de ciertas funcionalidades, o de la falta de otras, hasta la pregunta de ¿solución integrada y compacta, o productos especializados e independientes?.

Es un hecho que la incorporación de nuevas funcionalidades no siempre responde a las necesidades reales de seguridad, en ocasiones vienen a encarecer el producto, complicar su uso, a requerir más recursos de sistema, y a perjudicar el rendimiento global.

A su favor, estas soluciones compactas de seguridad evitan problemas de incompatibilidad e interferencias que pueden surgir entre productos independientes y terceras marcas, además de ofrecer una verdadera integración entre las diferentes funcionalidades desde un único interfaz, y un precio más ajustado en el caso de adquirir todas las funcionalidades en forma de productos independientes.

Si miramos a las redes corporativas se imponen los productos especializados, tanto en servidores como estaciones de trabajo. Para los servidores es vital contar con productos configurables según requisitos específicos, de alto rendimiento, estabilidad, y demostrada fiabilidad. En este perfil los productos “todo en uno” no encajan, además que es preferible no hipotecar toda la seguridad corporativa en un único producto o marca. Lo normal en estos casos es contar con varios productos independientes de casas especializadas en las distintas áreas: firewall, antivirus con más de un motor, IDS, etc., dotando al sistema de múltiples capas de protección independientes. En estos casos las dificultades de integración quedan compensadas con el resultado final, gracias a la labor de los administradores de sistemas y personal especializado en seguridad.

En las estaciones de trabajo corporativas podría parecer en un principio que encajan mejor las suites de seguridad compactas, si bien el problema en este punto se sitúa en la necesidad de productos sencillos, instalación distribuida, de configuración 0 para el usuario final, y de total administración centralizada y remota. Las últimas versiones de los antivirus con funciones extras dejan mucho que desear en este apartado (por ejemplo los que incorporan firewall personal), por lo que finalmente los administradores optan por la instalación de motores antivirus muy ligeros, que consumen pocos recursos para no tener problemas ante un parque heterogéneo de sistemas, y atendiendo a las facilidades de gestión en red.

Parece claro que el destino de las soluciones compactas está más ligado a los usuarios finales, si bien es necesario reinventar estos productos, ya que las necesidades de un usuario de a pie no se cubren adquiriendo e integrando tecnologías clásicas (firewalls, IDS, etc.), aunque tal vez sea éste el camino más cómodo y seguro para los desarrolladores, a corto plazo. Las casas de seguridad han de ser conscientes que este tipo de tecnologías clásicas vienen a requerir más conocimientos e interactividad por parte del usuario, quienes demandan todo lo contrario: algo que apenas se note y que no necesite de su atención.

Partiendo de la sencillez de instalación, configuración y uso de los productos compactos, es de esperar de estas soluciones una mayor adecuación a las necesidades reales de los usuarios finales (problemas de configuración, instalación de parches, criptografía aplicada a los mensajes y documentos, etc.), sin perder las posibilidades de personalización según cada perfil. Por ejemplo, partiendo de la compra de un

antivirus, poder adquirir módulos adicionales, según necesidades, a modo de plugins en línea. Lo que se traduciría en una configuración más ajustada, tanto en requerimientos, funcionalidades y precio.

Bernardo Quintero

28/04/2003 Virus, antivirus, y sensacionalismo mediático

A lo largo de la historia los creadores de virus han explotado los temas de máxima actualidad en sus especímenes, bien como reclamo para llamar la atención de los usuarios y conseguir así mayor número de infecciones, bien para aumentar las probabilidades de que su creación fuera motivo de noticia en los medios. Aunque la mayoría de las compañías antivirus procuran llevar una política seria de información sobre virus, en ocasiones también se han dejado arrastrar por el sensacionalismo en la búsqueda de una publicidad fácil, barata y, en la mayoría de las ocasiones, desproporcionada.

Hace unos días hemos podido asistir al último "virus mediático", en la forma de un gusano que aprovecha como reclamo la epidemia de neumonía atípica, simulando ser un mensaje con información relativa a esta enfermedad para engañar a los usuarios. Bautizado por las casas antivirus como "Coronex", se envía por e-mail utilizando diferentes asuntos y nombres de archivo con términos como SARS (Severe Acute Respiratory Syndrome) o Corona virus, haciendo referencia a la enfermedad de la neumonía atípica.

El gusano nunca habría salido a la luz por su peligrosidad, ya que no lleva a cabo ninguna acción dañina en los sistemas más allá de intentar propagarse, ni por su nivel de propagación, hasta el momento muy baja, tendiendo a nula según los indicadores de las propias casas antivirus. Sin embargo, hemos podido tener conocimiento de él a través de diversos medios, con titulares donde se mezcla la enfermedad de la neumonía con los virus informáticos, la única verdadera razón por la que se ha conocido.

En esta ocasión todas las noticias hacían referencia a la casa antivirus Sophos, que se ha encargado de "advertir" sobre este nuevo gusano. No deja de ser paradójico que en la nota publicada por Sophos se pidiera al resto de casas antivirus responsabilidad a la hora de informar sobre este gusano para evitar posibles confusiones. La realidad es que ellos han sido los únicos hasta el momento que han dedicado una nota especial a este espécimen, dando lugar a noticias sobre un gusano que, fuera del sensacionalismo mediático, no tendría que estar siendo motivo de noticia alguna.

Bernardo Quintero

13/06/2003 Microsoft y el mercado antivirus

El pasado martes, 10 de junio, Microsoft distribuía una nota de prensa donde anunciaba la adquisición de la tecnología antivirus de GeCAD Software, un peso pluma en el mercado de la seguridad. La expectación ante este movimiento es máxima, sobre todo entre las casas antivirus, a la espera de conocer las intenciones y planificación de Microsoft en este terreno.

La nota de prensa de Microsoft es lo suficientemente ambigua como para mantener la incertidumbre. Por un lado habla de aprovechar los conocimientos y experiencia de GeCAD para dotar a la plataforma de Windows de nuevas funcionalidades que aumenten y faciliten la integración de soluciones antivirus de

terceros, pero por otro lado no se descarta que Microsoft termine por ofrecer su propio motor antivirus basándose en el producto de GeCAD.

Si a esta última posibilidad se le une la tendencia de Microsoft a integrar en Windows los productos que pueden tener una competencia dominante en el mercado (recordar los casos de Internet Information Server o Internet Explorer), no es de extrañar el revuelo que la nota de prensa causó entre las firmas antivirus.

Experiencias anteriores
El escenario no sería nuevo, en 1993 Microsoft hizo una incursión en este mercado con MSAV (MicroSoft Anti-Virus) que distribuía junto a la versión 6.0 de MS-DOS. El antivirus de Microsoft era una versión de CPAV (Central Point Anti-Virus), un producto con solera en aquellos años que finalmente sería adquirido por Symantec.

El resultado fue nefasto, MSAV quedaba fuera de juego en poco tiempo por una mala política de actualizaciones que lo situó en clara desventaja respecto a sus competidores. En una comparativa realizada en enero de 1995, con la participación de más de 20 productos, MSAV quedaba en último lugar con resultados muy pobres en todos los apartados, incluyendo índices más que preocupantes en la detección de la colección In-The-Wild (los virus más extendidos).

En esa misma comparativa CPAV, que seguía su desarrollo y mantenimiento independiente a MSAV, consiguió resultados muy por encima a la solución de Microsoft. MSAV desapareció con la entrada en juego de Windows 95.

Extrapolando esta experiencia a la situación actual, Microsoft al menos puede estar seguro de que el antivirus de GeCAD no podrá superarle en ningún caso, ya que ha adquirido tanto el producto, RAV antivirus, como a su equipo de desarrollo y mantenimiento, incluyendo en el acuerdo cláusulas para impedir que puedan desarrollar otras soluciones antivirus. Con respecto a los problemas de actualización con que se toparon en MSAV, hoy día no sería mayor problema, teniendo en cuenta que Microsoft se ha convertido en el rey del parche con Windows Update y, además, ya cuentan con un público sumiso a la necesidad de las actualizaciones continuas.

RAV antivirus de GeCAD, ¿qué ha comprado Microsoft?

Definitivamente Microsoft no ha comprado tecnología de última generación, RAV es un antivirus clásico de detección por firmas, que no destaca por su innovación o funcionalidades proactivas. Eso sí, todo indica que en los últimos tiempos han inflado sus cifras incluyendo todo tipo de firmas, lo que en comparativas basadas en porcentajes de detección en colecciones zoo puede dar una falsa sensación de buen producto.

Particularmente no he evaluado RAV antivirus desde el año 2000, cuando participó en la comparativa de Hispasec de ese año, quedando fuera de la lista de los 10 mejores productos antivirus tras obtener un pésimo 17,32% de detección en la colección de troyanos.

Tras el anuncio de Microsoft he descargado e instalado la última versión de RAV, y lo que primero destaca es la cifra de más de 79.000 especímenes de malware que afirma identificar. Esta cifra tan elevada, muy por encima de productos destacados en el sector, apunta a que RAV es un claro exponente del "efecto zoo" (producto que artificialmente aumenta el número de virus detectados incluyendo firmas innecesarias con el único fin de alcanzar buenos resultados en comparativas, certificaciones y en la publicidad basada en números cuantitativos).

De las sospechas a las evidencias. Enfrentado contra una colección de falsos virus, RAV detecta muchas muestras que en realidad no pueden causar daño alguno, desde archivos dañados que no se pueden ejecutar, a los que RAV identifica con el sufijo "remnants", pasando por la detección de simples magazines sobre virus, herramientas clientes de seguridad y hacking, o muestras que suelen formar parte de las colecciones ZOO no depuradas, pero que en realidad no pueden ser clasificadas como malware.

Llegados a este punto, cabría preguntarse porqué Microsoft ha escogido a GeCAD. Bien porque se ha dejado llevar por los cantos de sirena de sus cerca de 80.000 virus que anuncia detectar, bien porque buscaba en la sección oportunidades y la empresa rumana era de las más baratas en comparación con otras que ya cuentan con un buen posicionamiento en el mercado, bien porque no quería irrumpir en el mercado como un elefante en una cacharrería y buscaba un peso pluma para no tener que elegir y decantarse por alguna de las grandes.

Si realmente lo único que quería era un antivirus clásico basado principalmente en la detección por firmas y su base de datos histórica, la elección en lo económico no es mala, ya que la tecnología es relativamente simple y similar en cualquiera de los productos y RAV/GeCAD debe ser con mucha diferencia la opción más barata que puede adquirir a día de hoy.

Si lo que pretendía era dar un vuelco a la seguridad de Windows con respecto a los virus y gusanos que les azotan, la compra del antivirus de GeCAD sirve de muy poco. Microsoft puede mejorar mucho en la lucha contra el malware si realiza modificaciones en la base, ya que presenta muchas debilidades por diseño. Pero integrar en Windows un antivirus basado en la detección de firmas supone un nuevo parche al ya de por sí parcheado sistema, y seguir un modelo de antivirus reactivo que día a día se muestra insuficiente para frenar a los especímenes que explotan el potencial de Internet para propagarse en cuestión de minutos.

¿Qué puede ocurrir?

Si finalmente la compra de GeCAD por parte de Microsoft sólo tiene como fin la investigación y desarrollo de nuevas funcionalidades en Windows que faciliten el trabajo de terceras casas antivirus, el mercado y los usuarios no deben de notar cambios bruscos. La vida seguirá igual.

Si por el contrario Microsoft pretende integrar el antivirus de GeCAD en Windows, queda claro que supondrá un duro varapalo para las firmas actuales. Bajo este escenario, las casas antivirus, en clara desventaja, sólo podrían competir (mejor dicho, adaptarse e intentar complementar al antivirus de Microsoft) innovando en nuevas técnicas antivirus más proactivas, productos especializados, y marcando diferencias en los servicios y tiempos de respuesta, donde a buen seguro serán mucho más ágiles y efectivos que Microsoft.

¿Mejoraría la seguridad del usuario?

Situándonos en el escenario más cambiante, la integración de un motor por detección de firmas en Windows, queda claro que supondrá la existencia de un antivirus en todos los sistemas Microsoft y que podría asegurarse su actualización con algún método agresivo (forzar la actualización automática, sin depender de la acción del usuario). En este punto la mejora parece evidente.

Pero si la entrada de un antivirus de Microsoft supone finalmente un claro predominio sobre el sector y la desaparición de la mayoría del resto de casas antivirus, el usuario está en peligro.

Por un lado la falta de competencia real, que hoy día está garantizada entre las diferentes firmas, supondría

un relajamiento en la necesidad de ofrecer respuestas inmediatas y mejoras en los productos. Por otro lado, el escenario de un antivirus común en todos los sistemas Windows da lugar a un sistema de seguridad muy homogéneo, que facilita enormemente la vida a los creadores de virus y permitiría epidemias más globales.

Mientras que hoy día un creador de virus debe diseñar su espécimen para que pueda burlar a una veintena de productos antivirus, cada uno con sus funcionalidades, firmas genéricas y heurísticas (cosa fácil, como demostramos en e-gallaecia), el día que reine un único producto en la mayoría de los sistemas sólo deberá dedicar "esfuerzos" (cosa de niños) para burlar esa protección a sabiendas de que afectará al 90% del parque mundial.

¿Podría Microsoft vender su antivirus sin integrarlo en Windows?

La posibilidad siempre existe, aunque la historia y la razón no apuntan hacia esa vía. También plantearía un dilema ético, que por un lado las debilidades de diseño de sus plataformas facilitaran la vida a los virus y que por otro se dedicara a vender la protección a su propia incompetencia.

En definitiva, finalmente deberemos esperar la jugada de Microsoft para ver como puede afectar esta adquisición a la situación actual de los antivirus, de momento todo son conjeturas e hipótesis.

Bernardo Quintero

28/09/2003 Impacto del monopolio de Microsoft en la seguridad

El dominio aplastante en el mercado de las soluciones de Microsoft, que se estima mantiene una cuota superior al 90% del parque mundial, es en gran parte el responsable de que las infraestructuras informáticas sean más vulnerables a virus y ataques. Esta es la conclusión a la que han llegado siete reconocidos expertos en seguridad, coautores de un informe que pone de relieve los peligros intrínsecos de las prácticas monopolistas y la falta de diversificación en los entornos informáticos.

Aunque el informe ha causado cierto revuelo en los medios de comunicación, sobre todo en EE.UU., los argumentos utilizados son bien conocidos en el mundo de la seguridad. Nada más conocer la publicación del informe, recordé un ejemplo muy gráfico que mi compañero Jesús Cea expuso hace 2 años en un congreso de seguridad, donde ambos analizábamos en nombre de Hispasec el grado de "culpabilidad" de Microsoft en la aparición de vulnerabilidades y epidemias de virus. Entre otros aspectos, salió a colación como la falta de diversificación aumentaba los riesgos de seguridad y facilitaba las infecciones masivas.

El ejemplo de Jesús Cea se situaba en el terreno de la agricultura, explicando como los monocultivos tenían importantes problemas cuando eran atacados por plagas o enfermedades, ya que el agente dañino se propaga rápidamente y afecta a la totalidad de la especie cultivada, aprovechando que se trata de una plantación homogénea con las mismas propiedades y puntos débiles. Por contra, los cultivos múltiples o policultivos, que intercalan la plantación de diversas especies sobre el terreno, son mucho más resistentes a las plagas y enfermedades, además de proporcionar otras ventajas en términos de estabilidad, rendimiento y productividad. La diversificación que establecen los policultivos actúan minimizando el impacto de las plagas y enfermedades, ya que el agente dañino se encuentra con especies a las que no puede atacar ni permiten su propagación, y en cualquier caso nunca afecta a toda la plantación.

A grandes rasgos, y en clave tecnológica, esta es una de las líneas argumentativas principales del informe "CyberInsecurity: The Cost of Monopoly". La analogía es tal que en una charla posterior, Will Rodger, director de la Computer and Communications Industry Association, comentaba que la situación actual, con Windows dominando en la mayoría de los PCs, era similar a las condiciones que se encontraron los granjeros durante el Hambre Irlandesa a mediados del siglo XIX.

Para los que no estén al tanto de esta crisis, por aquellos tiempos Irlanda tenía en la patata su principal fuente de alimentación. Una devastadora plaga entre 1845 y 1848 asoló en varias ocasiones los cultivos, lo que derivó en una época de hambre, enfermedades, muertes, y la catástrofe sumió a Irlanda en una profunda depresión en todos los ámbitos.

Como era de esperar la visión de Microsoft difiere totalmente. En palabras de Sean Sundhall, portavoz de la compañía, este tipo de analogías pueden ser más útiles para las patatas que para el software. Sundhall critica que el informe sólo señale los aspectos negativos de la monocultura en el sistema operativo, y sin embargo no mencione los positivos como la facilidad de mantenimiento.

Parche sobre parche

El informe, que no se basa en analogías con la agricultura, sino en hechos concretos y constatables de las políticas de Microsoft, también señala como el grado de complejidad que cada vez es mayor en Windows supone irremediablemente un aumento de los riesgos de seguridad.

Según este análisis, decisiones como la de incluir Internet Explorer de forma nativa en el sistema operativo, y convertirlo en parte integral y esencial del mismo, no responde a necesidades reales, sino a planes estratégicos y de mercado para castigar cualquier competencia en este terreno. Los riesgos de seguridad que esta decisión supone lo sufrimos regularmente, sólo hay que repasar los históricos de "una-al-dia" de Hispasec, incluido el último agujero crítico del navegador de Microsoft que data de primeros de septiembre y del que aun esperamos solución.

El número de vulnerabilidades en el que desemboca esta complejidad artificial adquirida por el sistema de Microsoft, con la integración de aplicaciones y funcionalidades en Windows que no obedece a necesidades básicas ni a la elección de los usuarios, lleva consigo una política de continuos parches para intentar corregir los problemas de seguridad. El informe recoge que este año llevamos 39 parches de Microsoft a día 16 de septiembre, a razón de parche cada 6 días. Un ritmo frenético para los administradores y profesionales, y casi una odisea para un usuario particular.

Además, el análisis mantiene que Windows ha llegado a tal punto de complejidad que la instalación de un parche para corregir una vulnerabilidad conocida tiene muchas probabilidades de introducir una nueva vulnerabilidad desconocida, un hecho que también hemos podido constatar en numerosos casos. A los riesgos de seguridad, hay que unirle los problemas de compatibilidad y estabilidad que las actualizaciones pueden acarrear, lo que a efectos prácticos supone que muchos usuarios y profesionales, temerosos de los efectos colaterales, retrasen la instalación de los parches hasta pasados unos días.

Protocolos y formatos cerrados

Otro de los frentes que utiliza Microsoft para controlar el mercado, también denunciado en el informe, es utilizar su posición de fuerza para implantar de forma unilateral estándares de facto, cuyos detalles mantienen ocultos, asegurándose su explotación.

Como ejemplos básicos que el usuario puede apreciar día a día, no son pocas las páginas webs que sólo se visualizan de forma correcta en Internet Explorer o que utilizan componentes que sólo pueden ser ejecutados bajo Windows. También hoy día es difícil encontrar una empresa privada u organismo público (lo que es más grave) que no utilice Microsoft Word como procesador de textos, incluido su formato propietario de documentos (.doc) tanto para el almacenamiento como intercambio de los mismos, en vez de utilizar formatos abiertos no dependientes de intereses privados.

En este tipo de situaciones los usuarios de otras plataformas no Windows se encuentran discriminados, hasta tal punto que para acceder a servicios de la administración pública se fuerza a utilizar las soluciones de Microsoft. Afortunadamente se está avanzando algo en este terreno, por ejemplo hoy día ya es posible acceder a los programas de ayuda de la Agencia Tributaria de España desde otras plataformas, aunque aun queda mucho camino por recorrer.

Polémicas sobre el informe

Algunas voces han querido poner de manifiesto una posible falta de imparcialidad en el informe, basándose en la participación de la CCIA (Computer and Communications Industry Association) en su presentación y publicación. Esta asociación de empresas integra, entre otras, a America Online, Oracle, o Sun microsystems, reconocidas competidoras de Microsoft. Además, la propia asociación tiene como fin la promoción de redes y sistemas abiertos, para garantizar la libre competencia, en clara oposición a la política de soluciones cerradas y las supuestas prácticas monopolistas de Microsoft.

Los autores han hecho hincapié en la independencia del informe, alegando que su origen parte de una iniciativa totalmente personal, que en ningún momento ha sido patrocinado por la CCIA o bajo los intereses de terceros. El documento viene firmado por Daniel Geer de @Stake (empresa a la que pertenecía hasta la publicación del informe), Charles P. Pfleeger de Exodus Communications, John S. Quarterman de Matrix NetSystems, Perry Metzger, consultor independiente, Rebecca Bace de Infidel, Peter Gutmann investigador del departamento de Ciencias de la Computación de la universidad de Auckland, y el reconocido Bruce Schneier de Counterpane Internet Security.

La CCIA también mantiene que su participación se ha limitado a la última fase, y que los autores se pusieron en contacto con ellos para dar la máxima difusión al informe, en especial para aprovechar sus recursos de cara a hacerlo circular en ambientes políticos y legislativos de Washintong.

También ha desatado ríos de tinta la salida fulgurante de Daniel Geer de @Stake, la que hasta ahora era su empresa, compañía de seguridad que tiene en Microsoft una importante fuente de ingresos. Desde @Stake aseguran que no han recibido ningún tipo de presión por parte de Microsoft, aunque tampoco esconden el malestar porque uno de sus trabajadores arremetiera públicamente contra un cliente tan importante, y se han dado prisas en desmarcarse de la opinión del mismo.

Buscando el equilibrio

Que Microsoft aprovecha su posición en el mercado es evidente, que los intereses comerciales se superponen a la seguridad de sus productos y que en la mayoría de las ocasiones son contrapuestos, también es constatable. De ahí a demonizar a Microsoft como origen y culpable de todos los males y problemas de seguridad que azotan a la informática actual, no parece razonable.

Mi opinión personal al respecto es que Microsoft es tanto víctima como culpable de la situación. Tener su sistema implantado en más del 90% del parque informático actual lo sitúan en el punto de mira de los

atacantes o de cualquier creador de virus, que siempre busca la plataforma más extendida para que su espécimen tenga un buen caldo de cultivo y que pueda obtener los mayores índices de propagación. Por tanto las vulnerabilidades de Microsoft, que en mayor o menor medida también podemos encontrar en otras plataformas, siempre tendrán una mayor repercusión en su caso.

Este papel de víctima no le exime de sus problemas específicos de seguridad, más aun cuando muchos de ellos han sido originados por la implantación de sus agresivas políticas de mercado que buscan asegurarse la explotación frente a terceros.

Por otro lado, es responsabilidad de los estamentos públicos y privados, sobre todo de los primeros, no someterse a la línea marcada por Microsoft o cualquier otra iniciativa interesada que no permita la libre competencia. Es muy importante ser conscientes de la importancia de adoptar estándares abiertos, de forma que las infraestructuras básicas, incluso el formato en que nuestros datos están almacenados, no dependan en exclusividad de un tercero.

Desde la competencia a Microsoft, de nada sirve apuntarle y criticarle de forma constante, si de forma paralela no se ofrecen soluciones que cumplan todos los requerimientos de los usuarios finales. No sólo de seguridad vive el usuario, la realidad es que no suele ser un factor clave que incline la balanza de la elección de un sistema operativo o aplicación, factores como la sencillez de manejo son mucho más valoradas por el usuario final. Es necesario un ejercicio de autocrítica que, al margen de las prácticas monopolistas de mercado ejercidas por Microsoft, permita reconocer sus aciertos y aplicarlos en las soluciones que se ofrezcan al usuario como alternativa al dúo formado por Windows y Office.

Con respecto al informe, es de lectura fácil y muy recomendable para todos los usuarios, que en última instancia deberán formarse su propia opinión. Se encuentra disponible en formato PDF en la siguiente dirección http://www.ccianet.org/papers/cyberinsecurity.pdf

Bernardo Quintero

13/10/2003 Microsoft: marketing vs. seguridad

En octubre de 2001 Microsoft lanzaba Strategic Technology Protection Program (STPP), que anunciaron como una iniciativa sin precedentes que mejoraría la seguridad de sus sistemas operativos y su respuesta ante nuevos problemas de seguridad. Pasados dos años, donde los incidentes de seguridad que aprovechan vulnerabilidades de Microsoft no han hecho más que aumentar, vuelven a realizar nuevas promesas.

De nuevo el marketing se adelanta a la tecnología. Durante una conferencia de partners la pasada semana, Steve Ballmer anunció nuevas iniciativas que harán de Windows un sistema menos vulnerable a los ataques. De entrada ha adelantado que estas funcionalidades se ofrecerán gratuitamente en el próximo service pack para Windows XP y Windows Server 2003. No sabemos si este anuncio debe interpretarse como que los usuarios de versiones anteriores de Windows, incluido Windows 2000, tendrán que migrar forzosamente si quieren acceder a este nuevo y prometido nivel de seguridad.

Además del anuncio público, de cara a mitigar el aluvión de críticas que está padeciendo Microsoft por el verano negro que ha protagonizado en materia de seguridad, tan sólo han transcendido vagas pinceladas sobre las medidas reales que implantarán. Desde la activación por defecto del firewall que incluye Windows, hasta una nueva política de avisos, parches y actualizaciones que pasarán a ser mensuales, en

vez de los más periódicos como nos tenía acostumbrado hasta ahora. Este último punto parece más una idea de un creativo de marketing que de un analista técnico. Desde el punto de vista de seguridad todo son desventajas. En palabras de Amy Carroll, director de producto de la unidad de negocio de seguridad de Microsoft, esta cambio facilitará a los usuarios la localización e instalación de las actualizaciones de seguridad.

Microsoft ha recibido en los últimos tiempos muchas críticas por los continuos parches de seguridad que deben aplicarse en Windows, lo que dificulta la labor a los profesionales y es poco práctico para los usuarios finales que no tienen porqué estar pendientes continuamente de las actualizaciones. Parece que Microsoft ha optado por simplificar el problema y reducirlo a lo absurdo: si no quieren muchos parches pequeños de forma periódica, daremos uno grande una vez al mes.
Los riesgos son evidentes, por un lado la ventana de tiempo entre que una vulnerabilidad es descubierta y la corrección está disponible será aun mayor, por otro lado los macro-parches, que tienen que modificar múltiples componentes del sistema, son más proclives a los problemas de compatibilidad e interferencias con el software ya existente.

Como anécdota, la misión principal de la iniciativa STPP era disminuir el tiempo que transcurre desde que es descubierta la vulnerabilidad hasta que el sistema del cliente es actualizado, y de esta forma disminuir el riesgo de que los sistemas resulten dañados. Ahora parece que dan la vuelta a la tortilla.

Como ya hiciéramos en su día en Hispasec, a través de la noticia “Microsoft STPP, ¿estrategia tecnológica o lavado de cara?”, de nuevo hacemos hincapié en que es una simplificación subjetiva y partidista del problema que sitúa al usuario como principal responsable al no actualizar periódicamente sus productos. A Microsoft le ha faltado de nuevo autocrítica en el planteamiento de la estrategia, y el anuncio de iniciativas encaminadas a corregir el problema en su origen. Más vale prevenir que curar.

Bernardo Quintero

Entrevista



Johannes B. Ullrich

Johannes Ullrich es el fundador de Dshield, que ahora forma parte de SANS Internet Storm Center, liderado también por él. En 2005 fue nombrado una de las 50 personas más influyentes en la industria de las redes por la revista Network World. En su trabajo diario suele usar Virustotal.

Hispasec: ¿Con qué edad empezaste a tener contacto con la informática? ¿Recuerdas los primeros equipos informáticos con los que pudiste trastear?

Johannes B. Ullrich: Tenía unos 14 años. La mayoría de los ordenadores con los que tenía contacto en el instituto era de Commodore. Por ejemplo tenía algunos Commodore 4004 (con 4 kylobytes de RAM y pequeños monitores verdes). En realidad aprendí bastante bien ensamblador 6502 que tenías que escribir en hexadecimal puro. Mi primer ordenador fue un Commodore 64.

H: ¿Cómo llega a convertirse un físico especializado en la investigación científica de rayos X, en un experto en seguridad informática e Internet?

JBU: Siempre me ha gustado jugar con los ordenadores. Mientras más me adentraba en experimentos

con rayos X, más importantes se hacían los ordenadores como herramienta para automatizar estos experimentos. Muchas de estas pruebas pueden llegar a ser aburridas si tienes que sentarte y esperar a que los datos se acumulen. Es mucho más divertido escribir un pequeño programa y dejar que el ordenador controle el experimento. Más tarde también empecé a controlar estos experimentos de forma remota a través de simples scripts CGI. Por supuesto, cuando empecé a trabajar con estos sistemas en red, me empezó a preocupar cada vez más la seguridad. Para algunas de estas simulaciones teóricas de estos experimentos, tomé prestadas varias estaciones de trabajo para planificar trabajos por todo el campus. De nuevo, esto me llevó a interesarme en cómo funciona realmente la autenticación y la reserva de recursos.

H: Para los que no conozcan a tu criatura, DShield, ¿puedes contar brevemente cuál es su objetivo y cómo ha ido evolucionando a lo largo de estos años?

JBU: Comencé Dshield como un “ISAC para usuarios normales” (ISAC = Information Sharing and Analysis Center). El término “ISAC” se usa desde 2000 para describir a las organizaciones de la industria que trabajan juntas para intercambiar información sobre seguridad. Por ejemplo, los bancos de Estados Unidos trabajan juntos en una ISAC. Leí sobre el tema y al mismo tiempo empecé a jugar con cortafuegos personales en casa. Supuse que a muchos usuarios caseros como yo les gustaría compartir información para tener una visión mejor de lo que realmente está pasando. Además, averigüé por amigos que trabajaban en ISPs que estaban absolutamente inundados de quejas relacionadas con el abuso del servicio.

Una de mis ideas era proporcionar a estos ISPs una forma sencilla y estándar de procesar estas quejas de abuso, las cuales están basadas la mayoría en muchos usuarios observando el mismo ataque, no sólo un individuo. Le di algunas vueltas a la idea y en noviembre de 2000 escribí mi primera versión del sitio durante un largo fin de semana. Lo ejecuté en un pequeño servidor que construí por unos 200 dólares y lo alojé en un ISP cercano que conocía. El primer problema fue encontrar un número de usuarios base para que introdujeran datos. Tuve suerte y Slashdot publicó la página después de un mes. Por supuesto la página se rompió y el ISP por poco me echa, pero al final, todo fue bien y conseguí mi “masa crítica” de suscriptores. En concreto, en 2001 estaba sorprendido con lo bien que funcionaba. Este fue un buen año de gusanos. Casi todos los encontramos pronto gracias a Dshield. Code Red fue particularmente interesante.

Mi primer pequeño servidor tuvo también sus problemas con este virus, mientras se introducían un montón de reportes y teníamos un buen número de visitas debido al interés de la prensa. La fuente de alimentación del servidor echó a arder pero tuvimos suerte y conseguimos seguir funcionando algunos días más hasta que puede reemplazarla (sólo se quemó algo de aislante).

H: Internet Security Center (ISC) es un referente para todos los que necesitamos tener información de última hora respecto a las amenazas que surgen en Internet. ¿Cómo está organizado internamente ISC para dar este servicio 24x7 y proporcionar siempre información relevante y contrastada?

JBU: Todos los “handlers” de ISC son voluntarios. Gracias a estos voluntarios podemos ofrecer el servicio. Todos tienen además trabajos reales. Como consecuencia, mucha de esa experiencia se cuela en nuestros “diarios”. Muchos servicios de seguridad profesional no tienen la misma experiencia en el mundo real.

H: Hemos podido comprobar que habitualmente en ISC, cuando se habla de amenazas de malware, se hace referencia a los resultados obtenidos en VirusTotal. ¿Qué opinión te merece VirusTotal y cuál crees que debe ser su evolución y papel en el sector de la seguridad?

JBU: Virustotal es una gran fuente para saber rápidamente si un malware es nuevo o no. Analizar malware lleva mucho tiempo, y recibimos muchos. Virustotal es una gran herramienta para clasificar y seleccionar rápidamente. Soy un gran fan del análisis automatizado del malware para hacerse una idea de lo que realiza el malware. Normalmente no es perfecto, pero algunos de los mejores sistemas pueden acercarse mucho a lo que en realidad ejecuta el troyano. Todo lo que podáis hacer en esa dirección sería muy interesante y apreciado.

H: Tanto DShield como ISC, o nuestro propio VirusTotal, parten de un enfoque donde se aprovecha la cooperación de la comunidad de Internet. ¿Cuáles crees que son las principales ventajas y retos de estos esquemas colaborativos que se nutren de datos distribuidos de terceras fuentes?

JBU: Internet es una gran comunidad. Tener una comunidad para investigar Internet tiene sentido. Una comunidad de voluntarios motivados puede resultar tremendamente poderosa. Por otro lado, seleccionar y motivar miembros responsables y con conocimientos para esa comunidad resulta un reto.

H: Esta entrevista formará parte de un libro que conmemora el décimo aniversario de una-al-día, el primer boletín diario de seguridad informática en español. No queríamos dejar pasar la oportunidad de aprovechar tu visión privilegiada en ISC para que nos resumieras brevemente tu opinión sobre cuál ha sido la evolución de las amenazas en Internet durante estos últimos 10 años.

JBU: El gran cambio es la "personalización masiva" de los exploits modernos. La década ha empezado con herramientas para automatizar la difusión de exploits. Incialmente teníamos simples herramientas para atacar manualmente sistemas y después, de nuevo gusanos simples pululaban por la red. Hoy, tenemos herramientas de ataques altamente flexibles y que escogen y seleccionan automáticamente exploits para que ataquen a un sistema en particular.

H: ¿Alguna predicción para el futuro en materia de seguridad en Internet? ¿Qué nos espera?

JBU: Con diseños de sistemas más complejos, como la virtualización y la "cloud computing", los ataques también se volverán más complejos. Creo que lo que veremos será nuevas formas de esconder malware en estos sistemas complejos. Por ejemplo en forma de virtualización "sigilosa" o procesos "inter-cloud".

H: Al margen de tu actividad profesional como Chief Research Officer for the SANS Institute,,¿a qué dedicas más tiempo últimamente? ¿Hobbies?

JBU: Estoy dedicando mucho tiempo a la seguridad web estos días. No hay demasiado tiempo para hobbies. De alguna forma, mi trabajo es mi hobbie ;-).

H: ¿Qué sistema operativo y navegador utilizas?

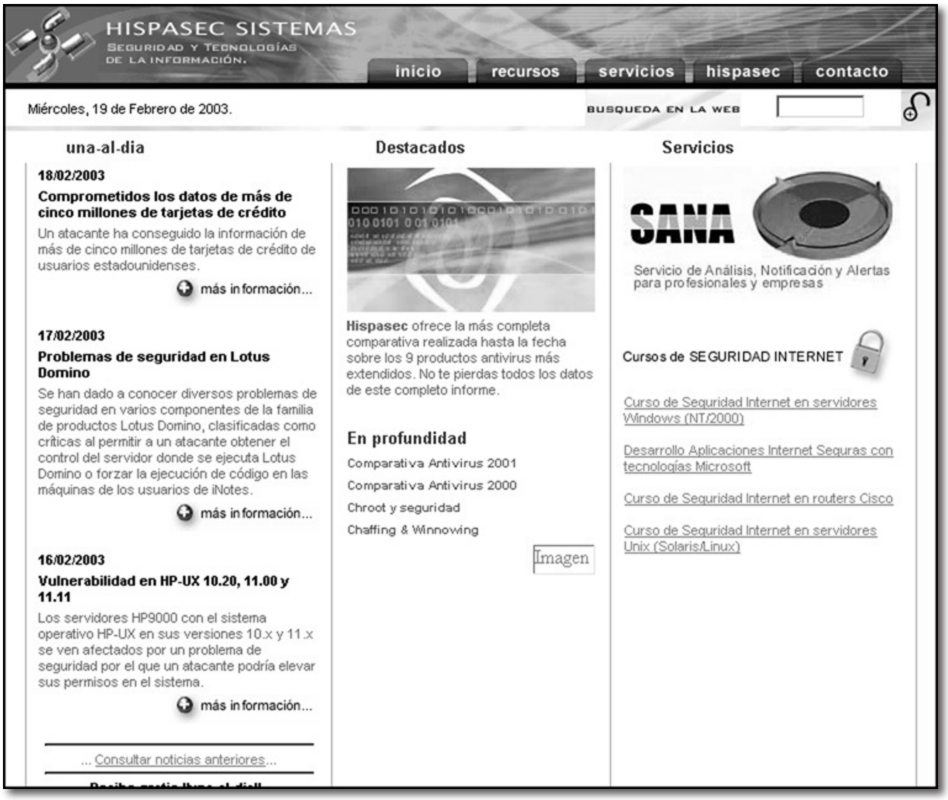
OS X y Firefox (también Safari). También uso Linux bastante.



H: Un libro, una canción

JBU: Sara Hickman, Mad World.
Duerrenmatt, The Physicists (mi libro favorito de todos los tiempos).

Página de Hispasec en 2003, tras la primera renovación



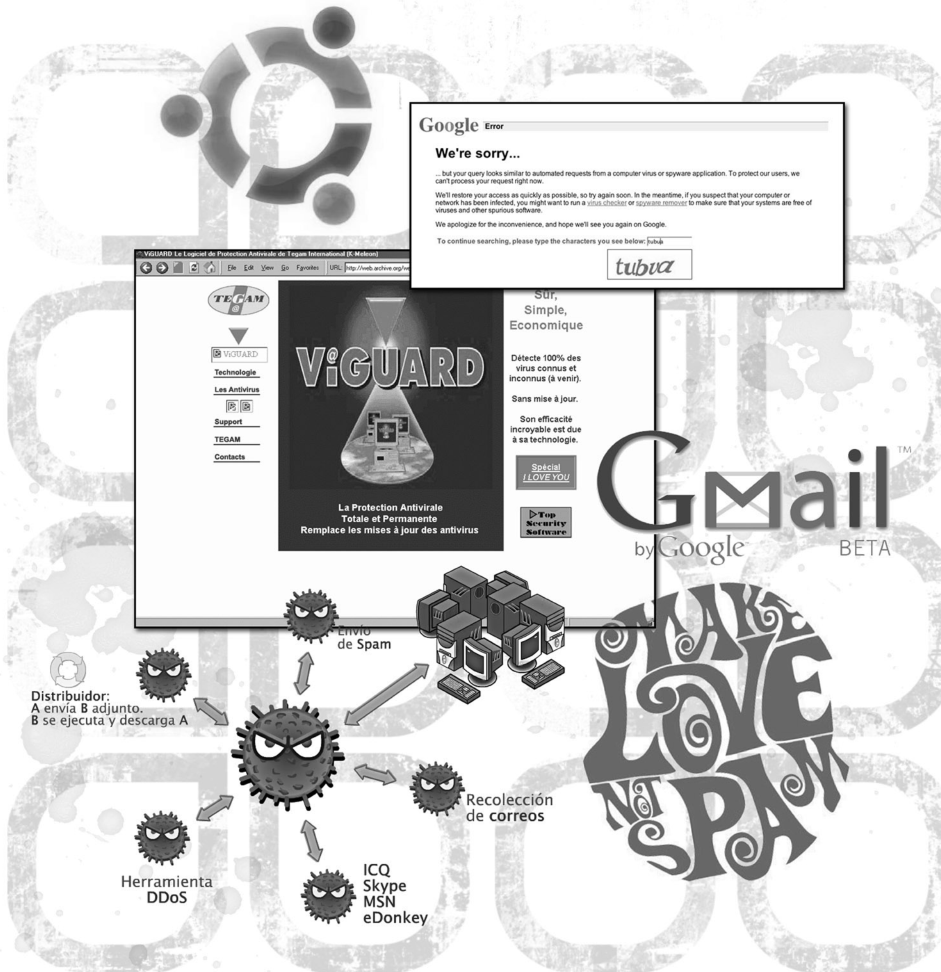
Capítulo 6

AÑO 2004

7D4

3724

11111010100



1073001600 – 1152748799



Durante este año...

_ En febrero la CIA admite que **no existía** amenaza inminente por las supuestas armas de destrucción masiva antes de la invasión de Iraq.

_ El 13 de febrero se pone en marcha en España el **Documento Nacional de Identidad (DNI) electrónico**. En 2008 se haría popular. Su implantación y uso en la Red es aún marginal.

_ Malta, Chipre, Estonia, Eslovenia, Letonia, Lituania, Eslovaquia, Hungría, República Checa y Polonia pasan a formar parte de la la **Unión Europea**. De la "Europa de los 15", se pasa a la "Europa de los 25".

_ **El Señor de los anillos**: El retorno del Rey, logra 11 Oscars, igualando el récord de Titanic y Ben-Hur.

_ El 2 de febrero, durante el espectáculo montado en el intermedio de la 38ª Super Bowl, **Justin Timberlake** interpreta "Rock your body" junto a **Janet Jackson** ante más de 100 millones de espectadores. Justin (en un supuesto movimiento de baile que pretendieron que resultara casual) arranca una parte del traje que oportunamente parecía sujeta con velcro y Janet deja ver su pecho derecho. Su interpretación de la sorpresa es más bien pobre, permite que se vea unos segundos e intenta ocultarlo con las manos. Este incidente, aunque se desmintiera hasta la saciedad que fuese algo preparado, sirvió como excusa para incluir cierto retraso en las emisiones en directo y poder estar preparados para "imprevistos", supuestamente de otra índole.

_ El 16 de febrero se descubre **una galaxia a 13.000 millones de años luz**, la más lejana conocida. Se consigue gracias a una combinación de observaciones del Telescopio Espacial Hubble y del observatorio Keck de Hawai.

Mueren 191 personas en los **atentados del 11 de marzo en Madrid**. Terroristas de nacionalidad marroquí colocan 13 mochilas con bombas en el interior de 4 trenes de cercanías que se dirigían a la estación de Atocha. Comienzan las especulaciones sobre la autoría de la masacre. Las elecciones se celebrarían sólo 3 días después, y durante el fin de semana los partidos políticos aspirantes se acusan de ocultar o exagerar información en beneficio propio. El 14 de marzo el PSOE gana las elecciones generales. El 15 de marzo Zapatero anuncia que retirará los 1.300 soldados que el país mantiene en Iraq.

El 3 de abril se produce la explosión en un inmueble de Leganés, habitado por sospechosos terroristas del atentado de Atocha. Muere un policía y siete terroristas se suicidan.

_ En los **Juegos Olímpicos de Atenas 2004**, el marroquí Hicham El Guerrouj gana las pruebas de 5.000 y 1.500 metros, algo que sólo había conseguido el finlandés Paavo Nurmi, en París en 1924.

El 1 de abril (el día de los inocentes anglosajón) Google anuncia por sorpresa su nuevo servicio de correo llamado **Gmail** que ofrecerá de forma gratuita a sus usuarios una cuenta con buzón de un gigabyte de capacidad. Muchos lo toman como una broma. La capacidad media de un disco duro en 2004 es de 60-80 gigas. Hotmail (quizás el servicio de correo más popular) ofrece en esos momentos gratis un buzón de dos megas, con la posibilidad de ampliar a 100 megas en el servicio de pago. Por si fuera poco, Google permite acceso a través de POP3 seguro con cualquier cliente. Gmail rompería así las reglas establecidas hasta el momento en el mercado del correo web. Ofrece durante muchos meses cuentas exclusivamente a través de invitaciones, pero no es complicado conseguirlas. Después el servicio se abriría para todos sin necesidad de invitación. Todos los servicios de correo comenzarían a aumentar el tamaño de sus buzones a pasos agigantados. El estándar establecido de "algunos megas" de forma gratuita para un buzón de correo se percibía ridículo de repente. No tardan en aparecer las utilidades que permiten usar esa capacidad extra integrada en el sistema operativo para salvaguardar datos de forma cómoda y remota, como si de una unidad local más se tratase. Gmail hoy día ofrece capacidad casi ilimitada y que aumenta cada día.

_ El 1 de septiembre el **colegio de Beslán**, en Osetia del Norte (Rusia) es secuestrado por terroristas musulmanes armados. Durante dos días retienen a cientos de personas en su interior, mientras sostienen armas y abundante material bélico. Se esconden bajo pasamontañas y portan numerosos explosivos. Toman como rehenes a 1.181 personas. Al día siguiente las conversaciones entre los negociadores y los secuestradores fracasan, negándose los terroristas incluso a permitir la entrada de alimentos y medicamentos para los rehenes, o a retirar los cadáveres del colegio. El día 3 de septiembre se produce un tiroteo entre los secuestradores y las fuerzas de seguridad rusas, dejando un saldo de más de 335 rehenes muertos (156 niños), 200 desaparecidos y cientos de heridos.

_ El 20 de septiembre la **Wikipedia** alcanza ya un millón de artículos en 100 idiomas.

_ El 20 de octubre se lanza la primera versión de **Ubuntu**. La 4.10 alias Warty Warthog. Ubuntu se convertiría en el "Linux para seres humanos" cuya filosofía es facilitar en lo posible el uso para escritorio. Supone un avance considerable en reconocimiento de hardware, drivers, etc, convirtiéndose en el abanderado del software libre en el entorno doméstico. En poco tiempo consigue una buena imagen, y copa el 30% de todas las instalaciones linux. Ofrece CDs oficiales gratuitos que pueden ser pedidos online y enviados a cualquier parte del mundo gratis. Basada oficialmente en el escritorio GNOME, más tarde aparecerían Kubuntu y Xubuntu, con el escritorio KDE y Xfce respectivamente. Su objetivo, como "fork" de Debian, sería proporcionar nuevas versiones cada 6 meses, algo considerado un problema en Debian, que en favor de la fiabilidad y estabilidad perdía "frescura" en su software.

_ En noviembre, **George W. Bush revalida su título** en la Casa Blanca batiendo al senador John Kerry.

_ En diciembre, **Symantec Corp** se funde con Veritas Software Corp.

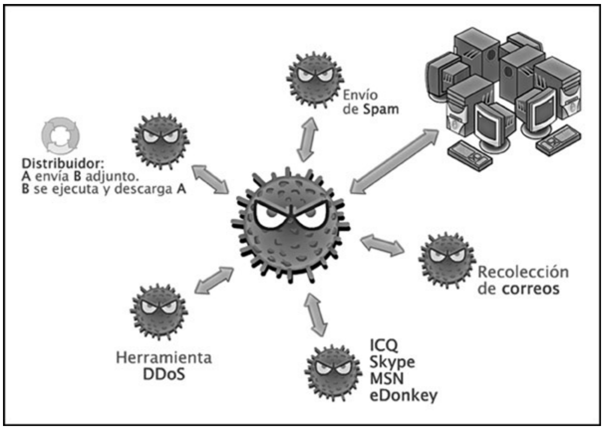
_ El 26 de diciembre se produce una de las mayores catástrofes naturales de toda la historia. Un tremendo terremoto de magnitud 9,3 sacude el sudoeste de Asia. El epicentro se encuentra en la costa oeste de la

isla de Sumatra. Su fuerza es tal, que genera un monstruoso **tsunami** que devora las costas cercanas de Tailandia, India, Sri Lanka, las Maldivas, Malasia, Myanmar, Bangladesh e Indonesia. Una gigantesca ola de decenas de metros de alto se introduce varios kilómetros tierra adentro, arrastrando y destruyendo todo lo que encuentra a su paso. Los muertos oficiales ascienden a 186.983 aunque más de 40.000 personas siguen desaparecidas hoy.

Seguridad Informática



_ A principios de año el grupo de trabajo de la IETF (responsable de la definición de las extensiones de seguridad en el protocolo DNS) solicita a la comunidad su opinión sobre los cambios propuestos para definir **DNSSEC**. No tendría mucho éxito. A raíz del problema descubierto en 2008, se replantearía con fuerza su uso más generalizado.



En enero aparece en escena **Bagle** y con él culmina la **"época romántica"** del malware para pasar a la era de la industrialización o malware 2.0. Su primera versión sentaba las bases de evoluciones posteriores que durante todo 2004 alcanzaría un nivel de sofisticación insospechado hasta la fecha. Los primeros Bagle tenían fecha de caducidad propia apenas 10 días después de ser lanzados. Se propagaban por correo electrónico. La versión B abría una puerta trasera en el puerto 8866. De forma periódica intentaba conectar con varios servidores HTTP, incluyendo en esa petición el puerto abierto en el sistema infectado y un identificador especial. Esto parecía ser un sistema de notificación ideado por el creador del virus para tener controlados los sistemas infectados (práctica habitual desde entonces). Las diversas variantes de Bagle, conjuntamente con otros gusanos con los que coincidió en el tiempo, provocarían por sí solos en los dos primeros meses de 2004 más actividad vírica que la registrada por todo el malware anterior durante todo el año 2003.

_ En enero Microsoft anuncia la firma de un acuerdo con el Gobierno español, que se adhiere así al **Programa de Seguridad para Gobiernos** (Government Security Program, GSP). Este acuerdo significa que los expertos en seguridad del Centro Nacional de Inteligencia (CNI), dependiente del Ministerio de Defensa, podrán acceder al código fuente de Windows, y a toda la información técnica que precisen para auditar las características de seguridad de la plataforma Windows. Poco después, y sin relación con el programa GSP, se filtran 660 megas de código fuente de Windows NT y 2000 en redes de pares con el nombre "windows_2000_source_code.zip"

_ En enero aparece otro malware clásico: **Mydoom**. Se distribuye también por correo electrónico. Cuando todavía no han transcurrido 48 horas desde la explosión del gusano Mydoom, se aprecia una segunda versión que apenas es reconocida por los antivirus. En febrero, el gusano Doomjuice aprovecharía

la puerta trasera de Mydoom para instalarse. Sus principales objetivos son atacar la web de Microsoft y realizar barridos de direcciones IPs buscando este puerto abierto. Cuando localiza uno, establece una conexión y envía una copia del ejecutable de Doomjuice, que el backdoor de Mydoom se encarga de recibir y ejecutar en el sistema. Comienza una guerra entre creadores de malware, que les lleva a dejarse mensajes sarcásticos en los códigos de los especímenes, aprovechar funcionalidades de otros e incluso desinfectar al usuario del malware "enemigo".

_ En marzo, **Netsky.P** es el más propagado del momento, y lo sería durante incluso años más tarde.

_ El 23 de marzo el equipo de **GNOME** hace pública una intrusión en sus sistemas informáticos. El personal técnico encargado de la administración de gnome.org comunica públicamente la detección de una intrusión en su servidor web. Todos los servidores gnome.org son desconectados inmediatamente, para evaluar la profundidad de la intrusión y evitar que los usuarios accediesen a información y código fuente comprometido.

_ En abril **Bagle** se alía con spammers para distribuirse junto a fotografías, una práctica que todavía perdura. El ancho de banda en los hogares aumenta, así que el gusano Bagle puede permitirse, entre otras formas de envío, simular ser un mensaje de una mujer y dotar a los correos con diferentes fotografías sugerentes, lo que lo dota de mayor realismo.

_ En mayo, **Sasser** infecta automáticamente sistemas Windows 2000 y XP vulnerables, convirtiéndose en una epidemia parecida a la que protagonizó Blaster. Aprovecha un desbordamiento de memoria intermedia en el servicio LSASS de Windows para infectar a otros sistemas de forma automática. Deja una puerta trasera que permite la intrusión a terceros. La propagación de Sasser en internet va en aumento exponencial, afectando a usuarios domésticos y servidores que no cuentan con las mínimas medidas de seguridad (con el puerto 445 TCP sin filtrar).

En mayo se da a conocer la historia de **Guillaume contra Tegam**. Un científico francés se enfrenta a una posible pena máxima de dos años de cárcel y multa de 150.000 euros, tras ser demandado por descubrir y publicar varias debilidades en el software antivirus de Tegam. En Hispasec se le da un especial seguimiento puesto que el resultado podría crear un importante precedente sobre la investigación independiente en materia de seguridad informática.



Guillaume publica en su página web personal bajo el apodo de "Guillermito", algunos análisis sobre vulnerabilidades que ha detectado en diversas soluciones de seguridad. El seudónimo es un guiño a sus raíces, puesto que sus abuelos eran españoles y migraron a Francia antes del comienzo de la Guerra Civil. En 2002 había publicado un análisis del antivirus francés ViGUARD (de Tegam International), en el que demostraba que la publicidad del producto era falsa al anunciar la detección del 100% de virus conocidos o no. Es más, realizaba sencillas pruebas que ponían muy en duda la eficacia del programa para la detección de muestras realmente simples. A raíz de sus investigaciones publicadas,

en octubre de 2003 Guillaume tuvo que responder a algunas cuestiones ante el grupo de la policía francesa que se encarga de los casos relacionados con las tecnologías de la información. También se vio obligado a acudir al Juzgado de Instrucción de París, atendiendo a la convocatoria de primera comparecencia sobre una acusación de Tegam International.

Se la acusaba de presunta "falsificación de programas informáticos y ocultación de estos delitos", escudándose para ello en varios artículos del código de la propiedad intelectual y el código penal. En un principio Tegam Internacional emprendió una agresiva campaña de marketing, con anuncios en publicaciones donde literalmente llamaba "terrorista informático" a "Guillermito". Acusación que cobraba una especial relevancia si tenemos en cuenta que apenas habían transcurridos unos meses desde el 11 de septiembre. El sitio web de Guillaume que hospedaba en un servidor francés desaparece junto con todo el que se había hecho eco de su estudio. Finalmente, tras el trabajo de su abogado, se retiran la mitad de los cargos esgrimidos contra Guillaume, pero debe afrontar los de "falsificación de información". El juicio, tras programarse para octubre, se retrasa hasta primeros de 2005. La historia seguiría.

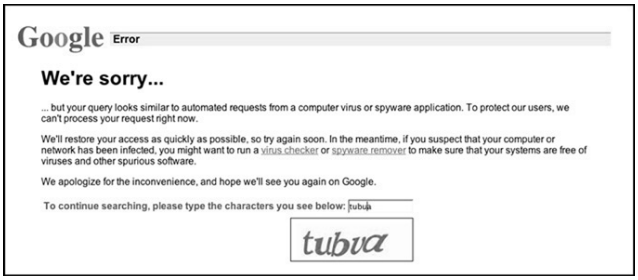
_ Del 31 de mayo al 4 de junio la ciudad de Santiago de Compostela acoge la **IV Semana Internacional de las TIC**, que comprende cuatro congresos internacionales: Seguridad Informática y Legislación en el Comercio Electrónico, Bases de Datos y Programación, Open Source, y Movilidad. Acuden **Bernardo Quintero y Julio Canto** con la conferencia "EL MAYOR ANTIVIRUS DEL MUNDO: VIRUSTOTAL". Sería la primera presentación pública de Virustotal.com, tras un desarrollo de un año.

_ En julio se anuncia la primera vulnerabilidad en **Gmail**. No se hacen públicos los detalles.

_ En julio, las nuevas versiones de **Bagle**, Bagle.AH o Bagle.AI (la denominación varía según el motor antivirus) consigue los mayores ratios de propagación.

_ El CERT/CC y el Servicio Secreto de los Estados Unidos publican un estudio que analiza los **ataques informáticos realizados desde dentro** de las empresas del sector bancario y fnanciero.

_ En verano, la nueva versión del gusano **Mydoom** destaca por realizar peticiones a los servicios de búsqueda de Google, Yahoo, Altavista y Lycos para recopilar direcciones de correo a las que enviarse. Algunos antivirus actualizan hasta 8 veces en una hora para poder hacer frente a la aparición salvaje de variantes. Son tantos los infectados que realizan peticiones de forma automática e involuntaria a los buscadores que caen varios servidores de Google. Necesita varias horas para restaurar la normalidad. Google se vio obligada desde entonces a instalar una medida de seguridad que, ante ciertas búsquedas sospechosas, pide al usuario un CAPTCHA para comprobar que no están siendo automatizadas. Hoy en día esa característica de Mydoom es todavía muy usada, gracias a que los atacantes han conseguido saltarse la seguridad proporcionada por los CAPTCHAS con sistemas automatizados.



_ La **Fundación Mozilla** ofrece una recompensa de 500 dólares por cada informe de vulnerabilidad en sus productos. Las condiciones son matizables. Sentaría precedente para otras campañas de recompensa por búsqueda y comunicación responsable de vulnerabilidades.

_ Aparecen grandes listas de aplicaciones incompatibles con el **Service Pack 2 para Windows XP**. El principal problema es que el Service Pack activa el cortafuegos entrante por defecto. Es el Service Pack que más modificaciones realiza sobre el sistema. Se trata prácticamente de una actualización de versión de sistema operativo. La seguridad de XP mejora considerablemente. Microsoft publica una herramienta para bloquear la instalación del paquete. Pasaría casi un año hasta que Microsoft volviese inefectiva esta herramienta y, aun instalada, obligara a la aplicación del Service Pack.

_ En septiembre, **Bagle** sigue campando a sus anchas sobre los sistemas Windows. Se detecta que la versión del momento no es un gusano (no se propaga por sí mismo), sino una especie de troyano que tiene como misión finalizar la ejecución de varios procesos de antivirus que pudieran estar activos en el sistema y desactivar el cortafuegos de Windows, para evitar así ser detectado. Además de intentar descargar lo que podrían ser nuevos componentes del gusano. Tiene como fuente 131 sitios webs distintos de Internet. Las características del malware 2.0 se consolidan.

_ En un movimiento similar al que adoptase Microsoft meses atrás, **Oracle** anuncia que distribuirá las actualizaciones de sus productos de forma mensual. Esta nueva política y los argumentos son exactamente los mismos que los que Microsoft estableció a finales de 2003 y que, en lo que a marketing se refiere, le da buenos resultados. Oracle recibe fuertes críticas. Durante más de 8 meses existían hasta 34 vulnerabilidades reconocidas por la propia compañía, que no ofrecía parche a sus clientes. El 31 de agosto publica el primero de sus superparches sin dar explicaciones ni detalles. Poco después Oracle ofrecería sus parches trimestralmente. La seguridad de Oracle es un desastre y no es hasta 2007 que comenzaría con tímidas mejoras para solucionar sus carencias en cuestión de seguridad.

_ En noviembre se detecta **Banker-AJ**. Únicamente se activa cuando el usuario visita determinadas sedes web de bancos ingleses, capturando las credenciales de acceso e incluso capturando las pantallas para conocer el estado de las cuentas corrientes. Banker-AJ representa una nueva evolución en el malware, altamente especializado y con un objetivo muy concreto. Cada días es más difícil definirlos como simples virus, gusanos, troyanos y otras variantes. La mayoría de los virus actuales utilizan las tácticas de los gusanos para su distribución y muchos troyanos pueden actuar como auténticos virus y sus funcionalidades son muy variadas. Banker se convertiría en toda una familia que, ante la imposibilidad de una ordenación coherente, albergaría cientos de miles de troyanos con estas características que aparecerían en el futuro. La banca online se convierte ya en objetivo preferente para el malware. Se siguen armando lentamente las piezas del panorama vírico actual.

_ En noviembre la versión de **Sober.I** se extiende por Europa. El gusano utiliza textos en alemán para enviarse por correo electrónico en caso de detectar que la dirección de destino pertenece a un país de habla alemana, utilizando el inglés para el resto.

_ En noviembre Hispasec publica un polémico estudio. Se refleja que el diseño de un 44% de las páginas **web bancarias españolas favorece el phishing**. El estudio está centrado en analizar los aspectos de diseño de la primera página web de las 50 principales entidades bancarias en España. Esta primera página de autenticación del usuario pueden permitir o facilitar el éxito de ataques phishing. Todas las entidades bancarias analizadas realizan correctamente la transmisión de datos de forma cifrada, sin embargo algunas de ellas, por motivos de diseño, usabilidad, etc. ocultan la url con HTTPS en algún frame, lo que dificulta a los usuarios la comprobación de que se encuentran en el sitio correcto. Un mes

después, más de un tercio de ellas han corregido sus deficiencias, quedando sólo 16 páginas “deficientes”. El dato es significativo teniendo en cuenta el corto espacio de tiempo transcurrido, lo que muestra la importancia e impacto que tuvo el estudio.



_ Después de semanas de críticas y una sonada campaña publicitaria, Lycos Europa decide suspender el polémico programa antispam titulado **“Make love not Spam”**. El programa consiste en la descarga gratuita de un salvapantallas para usuarios de Windows o Mac que cuando es activado envia peticiones inocuas a un servidor conocido de distribución de correo basura. Se busca que el efecto combinado de todos los salvapantallas descargados provoque una saturación de la máquina por congestión de tráfico. La polémica idea, tan criticada como alabada, pretendía alimentarse de bases de listas negras reputadas como Spamcop. Es rechazada por suponer una verdadera guerra “sucia” contra la basura. Pero se pone en marcha y al poco, Lycos sufre su propia medicina cuando un avispado spammer redirecciona los ataques hacia la propia página de la campaña makelovenotspam.com que cae durante horas. Lycos promete la vuelta del proyecto pero nunca se haría realidad.

_ El 15 de diciembre una-al-día comienza a estar también disponible a través de **RSS**.

Una al día



08/02/2004 Un 90% de las aplicaciones web son inseguras

Según un estudio realizado durante los últimos cuatro años por WebCohort, tan solo un 10 por ciento de las aplicaciones web pueden considerarse seguras ante cualquier tipo de ataque. En estos datos se incluyen sitios de comercio electrónico, banca online, B2B, sitios de administración, etc.

Los estudios realizados han concluido que al menos un 92% de las aplicaciones web eran vulnerables a algún tipo de ataque. Los problemas más comunes son las vulnerabilidades de cross-site scripting (80%), inyección SQL (62%) y falsificación de parámetros (60%). En las auditorías realizadas por Hispasec Sistemas también hemos podido comprobar como este tipo de problemas son más habituales de lo que cabría desear, lo que evidencia que la mayoría de las empresas no aseguran adecuadamente sus sitios web, aplicaciones y servidores contra cualquier tipo de intrusión.

La gravedad de estos problemas reside en como los ataques se realizan contra la propia aplicación web, el uso de las defensas habituales como firewalls, detectores de intrusos, etc. en la mayoría de los casos se muestran ineficientes. Los atacantes podrán acceder a datos de usuarios, de la empresa, detener sitios web, modificar la información del sitio web, e incluso llegar a ejecutar comandos en el servidor sin ser detectado en ningún momento.

Ya en el 2001, Gartner Group anunció que el 75% de los ataques informáticos a través de Internet eran realizados a través de las aplicaciones web. En la actualidad es fácil comprobar como persiste el mismo problema.

Antonio Ropero

15/02/2004 ¿Cuánto se tarda en resolver una vulnerabilidad?

En el momento en que se anunció la disponibilidad del parche para la vulnerabilidad en la biblioteca ASN.1 de Windows, los descubridores del problema mostraron públicamente su queja por el prolongado periodo de tiempo que transcurrió entre el descubrimiento y la disponibilidad del parche, especialmente teniendo en cuenta la criticidad del problema.

Cuando se publicó el reciente parche MS04-007, eEye (la empresa que había descubierto el problema) publicó un boletín con la descripción técnica el problema, como suele hacer.

Pero en esta ocasión, el boletín era ligeramente diferente. Para ilustrar el prolongado lapso de tiempo que transcurrió entre el descubrimiento y notificación del problema (finales de julio de 2003) y la disponibilidad del parche (febrero de 2004), eEye añadió un preámbulo al boletín con el texto de una canción.

Por si no fuera poco, eEye explicaba: “Nos hubiera gustado escribir un poema del tipo “Una noche antes de Navidad”, pero el fabricante ha dejado pasar algunas fechas, por lo que debemos de acudir a MC(SE) Hammer”. A continuación, publicaban la letra de la canción “U Can’t Trust This” (“No puedes confiar en esto”). Esta canción, por descontado, incluye un buen número de referencias a los diversos problemas de seguridad que ha sufrido recientemente Windows.

En varias ocasiones, desde Hispasec, hemos comentado el método tradicional (y no escrito) utilizado por la comunidad especializada en seguridad informática en lo referente al descubrimiento de vulnerabilidades. Así, tradicionalmente, se suele poner en preaviso a la empresa afectada, facilitando toda la información técnica y todos los detalles conocidos en primer lugar a la empresa y, en la medida que sea posible, colaborar en la resolución del problema.

Por su parte, el descubridor de la vulnerabilidad asume el compromiso moral de no desvelar la existencia de la misma hasta que el fabricante no distribuya públicamente la actualización necesaria para eliminar el problema.

¿Es normal tardar más de 28 semanas en publicar un parche para una vulnerabilidad tan importante como esta?

Se puede aducir, por parte del fabricante, que el desarrollo de una actualización no es una tarea trivial, ya que se hace necesario investigar y verificar que las modificaciones efectuadas no afectan negativamente al funcionamiento normal y esperado del producto. Igualmente, deben utilizarse unos mecanismos muy precisos para garantizar que las modificaciones efectuadas pasan a formar parte del repositorio oficial del producto (evitando, de esta forma, los problemas de regresiones).

Pero incluso asumiendo estos condicionantes que acabamos de citar, un periodo de 28 semanas (200 días) es muy difícil de justificar. Durante todo este tiempo Microsoft ha conocido la existencia de una importante vulnerabilidad de seguridad, que afectaba a un gran número de sus productos (incluyendo sus buques insignias) y que podía ser utilizada por atacantes remotos para ejecutar código de forma impune e incontrolable.

Otras vulnerabilidades

eEye parece que se ha cansado de esperar indefinidamente la respuesta de Microsoft a los problemas

que van descubriendo. Así, acaba de publicar una página de "próximos avisos", indicando la fecha de la notificación y el número de días que han transcurrido sin que Microsoft aporte una solución.

En esa relación de vulnerabilidades existentes y no solucionadas, por lo que cualquier intruso que conozca su existencia puede sacar provecho de las mismas, eEye avisa de la existencia de cinco vulnerabilidades críticas (aquellas que permiten la ejecución de código por un atacante remoto) que afectan potencialmente a varios centenares millones de usuarios. También se citan tres vulnerabilidades de severidad media y una vulnerabilidad de severidad baja.

Todas estas vulnerabilidades han sido convenientemente notificadas a Microsoft y el lapso de tiempo que ha transcurrido es, en el momento de redactar este boletín, entre 0 y 98 días. Sin llegar, de momento, al extremo recientemente vivido con la vulnerabilidad en la biblioteca ASN.1, a mi entender 98 días ya es un periodo de tiempo demasiado prolongado para una vulnerabilidad crítica.

Xavier Caballé

28/02/2004 Cambios en la arquitectura de los PC

En los últimos meses, han aparecido diversos anuncios sobre los cambios previstos en la arquitectura de los PC para aumentar la protección ante las incidencias de seguridad.

Hace ya más de veinte años, IBM presentó su primer ordenador PC con un procesador Intel 8088 a 4,77 MHz. Los ordenadores que hoy podemos encontrar en cualquier tienda de informática son una evolución de aquél diseño original, aunque básicamente los fundamentos continúan siendo los mismos.

En la actualidad existe un consorcio de empresas, la Trusted Computing Platform Alliance formado por Microsoft, IBM, HP, Intel, AMD y otros. Su objetivo es cambiar la filosofía básica de los ordenadores PC. Así, el PC dejaría de ser un equipo de propósito general donde es el usuario quien decide el software a ejecutar (o dispone como mínimo de la posibilidad teórica de decidirlo) para convertirse en una caja cerrada donde sólo puede ejecutarse aquél software que el fabricante ha autorizado expresamente.

Es decir, a grandes rasgos lo que pretenden estos fabricantes es convertir un PC en el equivalente a una videoconsola de juegos como las Playstation, Gameboy, Xbox y similares.

No obstante, en este boletín nos centraremos en dos cambios más próximos y que seguramente veremos en los próximos meses: la desaparición del BIOS y la incorporación de medidas de protección en los procesadores.

Desaparición del BIOS

El BIOS (Basic Input/Output System, sistema básico de entrada/salida) es el primer software que ejecuta el procesador en el momento de arrancar (o reiniciar) el ordenador, antes de la carga del sistema operativo. Su función básica es realizar un chequeo del ordenador y ofrecer acceso a los periféricos conectados al sistema. El BIOS es uno de los pocos componentes de la arquitectura de los PC que prácticamente no ha variado desde el primer PC.

Como sustituto del BIOS, Intel y Microsoft proponen una especificación denominada EFI (Extensible

Firmware Interface). El objetivo es permitir un arranque más rápido del ordenador. Adicionalmente permite realizar actividades como la identificación de la presencia de virus informáticos, especialmente aquellos que se instalan en el sector de arranque o modifican los archivos de inicialización del sistema operativo.

Mecanismos de protección en los procesadores

El siguiente cambio anunciado recientemente es la inclusión de mecanismos en los procesadores para evitar que los desbordamientos de buffer puedan ser utilizados para la ejecución de código. Básicamente consiste en que los datos que se encuentran en el buffer son considerados como de solo lectura y no puede ser ejecutado.

Los dos principales fabricantes de procesadores, Intel y AMD han anunciado de forma independiente la inclusión de estos mecanismos. No se trata, por descontado, de ninguna novedad. Ya hace años que los procesadores SPARC de Sun disponen de mecanismos similares.

Esta protección ya forma parte de los procesadores Athlon 64 de AMD actualmente disponibles. Por su parte, los futuros procesadores Prescott de Intel (nombre en clave de la versión mejorada del Pentium 4 con extensiones de 64-bit) incluirán algunas prestaciones similares.

Sin una protección de este tipo, un programa que no realice una comprobación adecuada de los datos introducidos por el usuario es susceptible de sufrir un ataque de desbordamiento de buffer. En este tipo de ataques, se envía una gran cantidad de datos, mayor de lo que inicialmente está previsto.

Como el área de memoria inicialmente reservada no puede almacenar esta gran cantidad de datos, éstos sobreescriben otras áreas de memoria. En determinadas circunstancias, este código puede ser controlado por el atacante para enviar código ejecutable que podrá ser utilizado de forma remota.

Es importante indicar, no obstante, que para sacar provecho de esta capacidad, el sistema operativo ha de incluir código para utilizar estas nuevas funcionalidades. No es algo que automáticamente pueda ser utilizado, sino que el sistema operativo que se ejecute debe activarlas.

Xavier Caballé

26/03/2004 Flecos de las soluciones antivirus

En plena oleada de gusanos informáticos son más evidentes los problemas que originan, como efecto colateral, algunas características de las soluciones antivirus. Aunque no dejan de ser incidentes que en teoría no afectan de forma directa a la seguridad del sistema, la realidad es que pueden desembocar en todo tipo de situaciones.

Uno de los problemas más comunes son los avisos que originan algunas soluciones antivirus para alertar y avisar a los remitentes de los mensajes infectados. En un principio podía considerarse una función útil, pero hace ya tiempo que la mayoría de los gusanos falsean la dirección de remite cuando se propagan. El resultado es que estas soluciones antivirus envían un mensaje alertando a una dirección de correo que en realidad no ha enviado el virus.

Muchos de nosotros habremos recibido algún que otro mensaje avisándonos de que hemos enviado un

virus y estamos infectados, cuando en realidad lo único que ha sucedido es que el gusano ha enviado desde otro ordenador infectado, que nada tiene que ver con nosotros, un mensaje con nuestro e-mail como remite falseado.

A partir de aquí se originan situaciones para todos los gustos. Desde aquellos usuarios que se creen el aviso y optan por apagar el sistema y buscar ayuda, hasta aquellos que escriben al destinatario para recomendarle que cambie de solución antivirus y que deje de alertar a los usuarios.

Además, por si no fuera poco con el spam y los propios gusanos, hemos de soportar el tráfico de esta nueva plaga de mensajes no deseados, que bien podríamos considerar también spam, no en vano los avisos suelen incluir el nombre del antivirus y un enlace. Primero te dicen que estás infectado, y luego te envían a la herramienta que lo detecta y desinfecta, no hay publicidad más directa.

La solución más simple pasa por que las soluciones antivirus no contemplen la funcionalidad de aviso a los remitentes de mensajes infectados. Otra opción, más elegante, y que permite mantener la utilidad de las notificaciones, es que los antivirus no realicen el aviso de forma indiscriminada, como hasta ahora, sino que sólo lo hagan en el caso de virus, troyanos, o gusanos que no realizan la falsificación del remitente, algo muy fácil para ellos, ya que les basta con incluir una simple marca en las firmas de detección para reconocer en que casos no deben avisar.

Otro de los efectos colaterales más comunes se detecta en aquellas soluciones antivirus de servidor de correo que desinfectan el archivo adjunto infectado pero que dejan pasar el mensaje del gusano, a veces con parte de los archivos adjuntos incluido. Son muchos los usuarios que se alertan al recibir este tipo de mensaje, ya que creen que se trata de mensajes infectados, y reclaman a los administradores de sistemas.

Como anécdota, una importante organización ha enviado recientemente un comunicado a todos sus usuarios avisándoles que los mensajes en inglés que reciben ya han sido desinfectados, en un intento de tranquilizarlos y evitar las continuas alarmas. La realidad es que la solución puede ser peor que el problema, ¿qué ocurrirá cuando de verdad se les cuele un gusano por el antivirus perimetral? ¿los usuarios creerán que es inofensivo porque ya ha sido desinfectado?

De nuevo la solución está en manos de las casas antivirus, ya que es muy fácil mantener una lista o una marca en las firmas de virus para reconocer los gusanos “puros”, especímenes que crean todo el mensaje y se autoenvían. En estos casos de gusanos “puros” la solución antivirus debería eliminar por completo, tanto el archivo adjunto como el mensaje, y que el usuario (destinatario) no reciba absolutamente nada, evitando cualquier tipo de confusión y un tráfico totalmente innecesario.

Bernardo Quintero

03/05/2004 Gusano Sasser: un mal menor que evidencia la falta de seguridad

Cuando aun nos encontramos en plena epidemia, con la aparición en las últimas horas de una cuarta variante, podemos afirmar que el gusano Sasser ha sido un mal menor. Todas las máquinas infectadas permitían a un intruso obtener el control total sobre ellas, desde la posibilidad de sustraer datos sensibles como documentos privados o las claves de la banca electrónica del usuario, hasta borrar todo el sistema local y unidades de red.

A nadie escapa los quebraderos de cabeza que Sasser está ocasionando tanto en sistemas domésticos como, especialmente, en redes corporativas. Si bien, afortunadamente, el gusano sólo estaba programado para reproducirse, sin llevar a cabo ninguna acción adicional.

Si el creador del gusano hubiera introducido una simple línea más de código con algunas instrucciones dañinas, algo que no requiere ningún esfuerzo técnico especial, podríamos estar en estos momentos en una catástrofe sin precedentes que probablemente traspasaría la barrera de lo estrictamente informático, por la cantidad y sensibilidad de los procesos y datos a los que habría podido afectar. Pensemos por un momento que simplemente hubiera borrado todas las unidades a las que tenía acceso en cada uno de los ordenadores infectados.

En ningún caso pretendo minimizar el daño causado por el autor del gusano, de proporciones incalculables y que no tiene justificación alguna. En estos momentos ya hay varias investigaciones en paralelo para localizar el origen y llevar al autor ante la justicia. Si bien, es necesario llevar a cabo un ejercicio de autocrítica más allá de culpar exclusivamente al creador del mismo y ser conscientes del riesgo real que entraña no instalar puntualmente los parches, no en vano está en juego la seguridad de todos los datos y procesos dependientes de nuestros sistemas. ¿Podemos permitirnos arriesgarlos de nuevo?

La historia se vuelve a repetir, una y otra vez.

Code Red y Nimda en el 2001, o SQL/Slammer en el 2003, han sido claros exponentes de gusanos de propagación masiva que aprovechaban vulnerabilidades en los productos de Microsoft para propagarse de forma automática. Mucho más peligrosos que los típicos gusanos que se propagan por el correo electrónico, que requieren que el usuario los abra y ejecute para poder activarse.

Sin ir más lejos, en agosto de 2003 asistimos a la epidemia global causada por el gusano Blaster, que aprovechaba una vulnerabilidad en un servicio estándar de Windows, prácticamente un calco a lo que está ocurriendo con Sasser.

El patrón se repite. Gusanos de red que aprovechan vulnerabilidades, cuyos parches para corregirlas y prevenir la infección estaban disponibles con antelación. En todos los casos, desde Hispasec advertimos por este mismo medio del riesgo potencial que entrañaba no instalar dichos partes, incluso pronosticando la aparición de gusanos.

Llegados a este se puede discutir el grado de responsabilidad de Microsoft en el origen de las vulnerabilidades, su política de distribución de parches, esperar a que incorpore y active por defecto un firewall personal, barajar la posibilidad de migrar a otro sistema operativo con menos índices de virus y gusanos, o la necesidad de que los antivirus cambien su modelo reactivo que a todas luces es más que insuficiente contra este tipo de gusanos, capaces de infectar miles de sistemas en cuestión de minutos.

Otra opción, que no excluye todo lo anterior y a muchos más factores, es empezar por hacer autocrítica constructiva, y que los afectados asuman su buena parte de responsabilidad de cara a prevenir futuros incidentes.

Actualizar los sistemas, tan simple como efectivo

Dejando al margen comparaciones sobre el número de vulnerabilidades críticas que periódicamente afectan a Microsoft, los usuarios de Windows deben ser conscientes de que se trata de un producto que debe ser actualizado regular y puntualmente, como todos los sistemas operativos, en mayor o menor

medida. Es necesario realizar una campaña de concienciación/educación sobre la necesidad de mantener actualizados los sistemas, de las herramientas y servicios automáticos que existen para facilitar esta tarea, y de los riesgos que entraña no seguir esta práctica.

Ya no sólo para evitar infecciones de gusanos como Sasser, o de efectos peores. Sino que los usuarios deben ser conscientes de que, cada vez que no instalan un parche crítico, están dejando una puerta abierta para que un intruso pueda controlar totalmente su sistema, sustraer su información más sensible, borrar sus discos duros, o espiar todo lo que hacen con su ordenador. Y esto ocurre con mucha más frecuencia de la que se cree, con el agravante de que suele pasar desapercibido, al contrario de lo que ocurre con los gusanos.

En el ámbito corporativo todo lo anterior es aplicable. En Hispasec observamos, durante las auditorías de seguridad a sistemas corporativos, como suele existir una atención especial en la protección perimetral y de los servidores con servicios en Internet, dejando en un segundo plano, a veces olvidado, al resto de servidores internos, y especialmente a los PCs que actúan como estaciones de trabajo.

Es un grave error, de hecho toda la información sensible pasa por las estaciones de trabajo, que en la mayoría de las ocasiones podría estar bajo el control de un atacante gracias a las vulnerabilidades que poseen.

Otro talón de Aquiles típico en las políticas de seguridad son el control de los dispositivos móviles de uso personal, como portátiles, o usuarios de acceso remoto. En la mayoría de los casos se tratan de sistemas que se encuentran más expuestos a los riesgos de seguridad, ya que no siempre están bajo el paraguas de las protecciones corporativas. Sin embargo estos sistemas pueden llegar a tener una estrecha relación con la red interna, siendo en muchos casos el origen de las infecciones.

Bernardo Quintero

01/06/2004 El mayor antivirus público de Internet

VirusTotal es un nuevo servicio de detección de virus, gusanos y malware en general, que permite analizar archivos con múltiples motores antivirus. Cualquier usuario de Internet puede enviar archivos o mensajes sospechosos y obtendrá de forma gratuita un informe con el resultado del análisis.

Desarrollado por Hispasec Sistemas, con la colaboración de Red.es y Jazztel en el soporte del ancho de banda del servicio, VirusTotal fue presentado ayer durante la Semana Internacional de las TIC, que se celebra en Santiago.

VirusTotal integra los motores antivirus de Computer Associates (etrustAV), Eset Software (NOD32), FRISK Software (F-Prot), Kaspersky Lab (Kaspersky), Network Associates (McAfee), Norman (Norman), Panda Software (Panda Platinum), Softwin (Bitdefender), Sybari (Antigen), Symantec (Norton Antivirus) y TrendMicro (PC-Cillin). Adicionalmente a estos antivirus, Hispasec está trabajando en la incorporación de nuevos motores que aumentarán, más si cabe, la capacidad de detección del servicio.

En la dirección http://www.virustotal.com los usuarios podrán acceder al formulario de análisis, a estadísticas globales en tiempo real sobre incidencias, así como a descripciones e información sobre virus y malware en general.

Además, los usuarios pueden reenviar directamente los mensajes o adjuntar los archivos sospechosos mediante correo electrónico a la dirección analiza@virustotal.com con el asunto ANALIZA. En breves instantes, dependiendo de la carga puntual del servicio, recibirán en su buzón el informe detallado del análisis.

El tiempo de respuesta dependerá del número simultáneo de usuarios que utilicen el servicio, que podría ser notablemente superior durante los primeros días de la publicación de VirusTotal, si bien se espera se estabilice a finales de esta semana.

Hispasec quiere hacer hincapié en que VirusTotal no sustituye de forma alguna a los antivirus instalados en los PCs, ya que sólo permite el análisis a demanda de archivos individuales, y no ofrece protección permanente al sistema del usuario. Este servicio está destinado principalmente a facilitar el análisis de archivos o mensajes sospechosos que, aun siendo dañinos, no sean detectados por el antivirus utilizado por el usuario, bien porque se trata de un espécimen muy reciente aun no incorporado a sus actualizaciones, bien por cualquier otra circunstancia.

También es importante señalar que, pese a que el índice de detección ofrecido por el análisis simultáneo de múltiples motores antivirus es muy superior al de un sólo producto, los resultados no pueden garantizar la inocuidad de un archivo. No existe solución en el mundo que pueda ofrecer un 100% de efectividad en el reconocimiento de virus y malware en general.

Por último, Hispasec quiere agradecer la colaboración y el apoyo mostrado por las casas antivirus participantes en VirusTotal, así como animar a los usuarios a que prueben el servicio.

Hispasec Sistemas

24/10/2004 Informe: comparando la seguridad de Windows y Linux

La publicación inglesa “The Register” publica un informe donde se analiza el modelo de seguridad utilizado por Windows y Linux, intentando determinar las diferencias entre ambos. Se trata de un intento de sistematizar los puntos fuertes y débiles de cada entorno y, con esta información, intentar extraer unas conclusiones.

Una discusión recurrente en los últimos meses trata sobre que es más seguro, si el software propietario o el software de código abierto. Los defensores del primero defienden que la disponibilidad del código fuente abre la posibilidad que los atacantes descubran nuevas vulnerabilidades. Por su parte, los defensores del software de código abierto afirman que justamente la disponibilidad del código es la mejor receta para evitar los problemas de seguridad.

Se trata de una discusión en la que habitualmente se suelen utilizar, por ambos lados, argumentos que huyen de los datos empíricos y demostrables. Generalmente se utilizan argumentaciones de carácter sentimental y apreciaciones subjetivas, que poco ayudan a mantener un debate sosegado y que realmente permita extraer conclusiones.

El informe, “Security Report: Windows vs Linux” empieza con el análisis de tres mitos frecuentemente utilizados en cualquier discusión donde se compara la seguridad de Windows y Linux.

El primer mito es que Windows es objeto de más ataques y es víctima de la acción de más virus y gusanos debido a su posición dominante en el mercado. Dado que Windows es la plataforma dominante, los autores de ataques y virus tienen preferencia por esta plataforma. El informe rebate este mito a partir de dos datos empíricos: Linux es una plataforma muy popular a nivel de servidor Web y los datos recogidos por Netcraft demuestran que máquinas ejecutando software de código abierto no son reiniciadas con frecuencia.

El segundo mito se refiere a que la disponibilidad del código fuente abre la posibilidad a descubrir más fácilmente las vulnerabilidades. Este argumento se rebate a partir de la enorme cantidad de gusanos y virus que sacan provecho de vulnerabilidades de Windows, lo que viene a demostrar que la disponibilidad del código fuente no es un factor clave para detectar la existencia de problemas de seguridad.

El tercer mito rebatido son las estadísticas que demuestran la existencia de menos problemas de seguridad críticos en la plataforma Windows con respecto a Linux. En el informe se facilitan datos que demuestran como muchas de estas estadísticas son confeccionadas a medida y se basan en datos parciales, que difícilmente se pueden extrapolar a las conclusiones que a veces se extraen de los mismos.

La segunda parte del estudio compara el diseño de Linux y Windows, analizando las implicaciones que tienen las mismas en lo relativo a la seguridad. Así se compara el diseño monolítico de Windows contra el diseño modular de Linux (no se refiere al núcleo del sistema operativo, sino al conjunto del sistema operativo), el origen del código, las limitaciones del modelo de llamadas de procedimiento remoto y la diferencia de orientación de los ambos productos.

En la tercera parte se analizan las métricas utilizadas para la medición del nivel de seguridad y la dificultad que supone la interpretación de los datos reflejados por las mismas.

Cuando se mide el nivel de seguridad no sólo deben considerarse factores puramente numéricos, como son el número de vulnerabilidades sino que otros elementos tienen una importancia igual o superior: la exposición potencial a la vulnerabilidad, la facilidad con la que las vulnerabilidades pueden ser utilizadas en ataques, el daño provocado como consecuencia de un ataque. La unión de estos factores permite identificar un nivel de riesgo.

Con todas estas consideraciones, el informe realiza una comparativa de los últimos cuarenta parches y actualizaciones de Windows Server 2003 y Red Hat Enterprirse Linux AS v3.0. Se realiza una tabulación en la que se aplican las métricas definidas, de forma que para cada vulnerabilidad se puede identificar el nivel de riesgo global.
También se facilitan datos obtenidos a partir de la valoración global de impacto que aplica el CERT a cada una de las vulnerabilidades que se publican.

Conclusiones

Aplican las métricas definidas por "The Register", el impacto de las vulnerabilidades y actualizaciones es mucho más importante en Windows Server 2003. Aproximadamente la mitad de las actualizaciones de Microsoft son consideradas como críticas (y muchas de las que no tienen esta consideración es debido a la configuración particular de Internet Explorer y Outlook Express, que son difícilmente utilizables en su configuración por defecto).

En cambio, aplicando la valoración que añade el CERT en sus estadísticas se puede considerar la existencia de un "empate tácito" en el nivel de seguridad de Windows Server 2003 y Red Hat Linux Enterprise Linux AS v3.0, con una valoración ligeramente favorable a Windows.

Xavier Caballé

Entrevista


Bruce Schneier

Bruce Schneier es el criptógrafo y gurú de la seguridad por excelencia. Desde la publicación de su libro "Applied Cryptography", un referente en cuestión de seguridad de todos los tiempos, ha ganado una merecida reputación que le define como una de las personas más lúcidas en el campo de la criptografía y de la seguridad. Especialmente en el impacto que estas disciplinas ejercen sobre la sociedad real. Un gran comunicador que ha accedido a responder a algunas de nuestras preguntas.

Hispasec: ¿Con qué edad empezaste a tener contacto con la informática? ¿Recuerdas los primeros equipos informáticos que pudiste trastear?

Bruce Schneier: Mi primer ordenador fue un mainframe en mi universidad. Mi instituto tenía un terminal, y los programas se guardaban en tarjetas perforadas. El primer ordenador que tuve era el primer Apple de Macintosh.

H: ¿Cuándo descubres por primera vez la criptografía? ¿Por qué decides dedicarte a ello profesionalmente?

BS: Siempre me ha interesado la criptografía, incluso de pequeño. Trabajé para el Departamento de Defensa de Estados Unidos cuando me gradué en la universidad, y decidí escribir [el libro] Applied Cryptography después de ser despedido de AT&T Bell Labs en 1991.

H: La criptografía ha sufrido grandes avances desde 1998, pero también han avanzado los tipos de ataque. ¿Crees que la criptografía es ahora mejor que hace diez años?

BS: Sabemos mucho más de criptografía que hace 10 años. Muchas de las mejoras están ya bordeando los límites y podrían no ser perceptibles para alguien ajeno a este campo, más que nada porque hemos tenido toda la criptografía que necesitamos y los problemas serios están en la seguridad de las redes y los ordenadores. Pero las mejoras son reales: el campo de la criptografía continúa avanzando.

H: ¿Puede un algoritmo criptográfico por sí sólo garantizar la seguridad de una operación o siempre dependeremos en última instancia de otros factores como el humano?

BS: La criptografía es matemáticas, y la criptografía puede garantizar la seguridad de las matemáticas. Por desgracia eso no es muy interesante: la seguridad solo es importante cuando interactúa con la gente. Y una vez que la seguridad implica a las personas, las personas van a ser el mayor riesgo de seguridad. Así que no: mientras la criptografía pueda asegurar un correo de un ordenador a otro, nunca podrá asegurar el enlace que existe entre el teclado/pantalla y la silla.

H: Aunque el algoritmo MD5 se considera "muerto" en términos criptográficos, vemos que aún sigue vigente en muchos sistemas y soluciones de seguridad. ¿Por qué parece que cuesta tanto migrar a algoritmos más seguros? ¿Falta de conciencia?

BS: MD5 hace tiempo que fue oficialmente reemplazado por SHA. SHA ha sido oficialmente reemplazado por SHA-1. Y SHA-1 ha sido oficialmente reemplazado por la familia de algoritmos SHA-2. Estos serán reemplazados sobre 2012 por SHA-3, un algoritmo todavía por determinar. La National Institute of Standards and Technology mantiene un concurso para elegirlo. Estoy orgulloso de mi propia propuesta para este proceso, llamada Skein (madeja).

Así que todo el que todavía esté usando MD5, o bien no está prestando atención o no le preocupa actualizarse. Y ese es el problema con sistemas heredados: están estancados con seguridad que estaba bien cuando se crearon pero que ya no son adecuadas.

H: Ante el problema del phishing, muchas entidades bancarias están implantando sistemas de autenticación de doble factor, con el uso de SMS a teléfonos móviles, certificados digitales, smartcards, tokens, incluso en España se está utilizando un documento de identidad electrónico (e-DNI) expedido por el gobierno. Sin embargo, nosotros estamos viendo como muchos troyanos bancarios actúan modificando la cuenta de destino y la cantidad en las transferencias de forma transparente al usuario una vez éste ya se ha autenticado en el sistema, haciendo inútiles este tipo de medidas. ¿Qué deberían hacer las entidades bancarias para proteger a sus clientes?

BS: Escribí sobre esto cuando la autenticación de dos factores comenzaba a hacerse popular... que no haría nada para detener el fraude bancario online. El fallo está en que la autenticación de dos factores tiene como objetivo la táctica, no el problema en sí. Así, como habéis notado, los atacantes solo han tenido que cambiar sus tácticas. La solución es intentar dejar de autenticar a la persona y empezar a autenticar la transacción. Esa es la forma en la que las compañías de tarjetas de crédito previenen el fraude, y es lo que funciona.

H: En el mercado de la seguridad, ¿cuánto hay de marketing, cuanto de snake-oil y cuánto de seguridad real? ¿Qué recomendaciones darías a los usuarios finales y a los responsables de seguridad corporativa para que no se dejen llevar por el marketing y elijan soluciones efectivas?

BS: Es una causa perdida. La seguridad se ha vuelto tan complicada que el comprador medio ya no puede entender lo que el vendedor medio le está vendiendo. Así que los vendedores recurren al marketing a costa de la "sustancia". Mi consejo es hacer "ousourcing" tanto como sea posible y especificar las métricas de seguridad en el contrato. Deja que otro se preocupe por los detalles técnicos y concéntrate en los resultados.

H: Mirando hacia atrás, la historia nos dice que el criptoanálisis triunfó en muchas ocasiones sobre la criptografía del momento, que a nivel militar y gubernamental se dedicaban muchos recursos a esta tarea, y que algoritmos que por entonces se creían robustos en realidad estaban siendo comprometidos. ¿Sería lógico pensar que puede estar ocurriendo lo mismo con los algoritmos actuales?

BS: Por supuesto los sistemas criptográficos están siendo comprometidos todo el tiempo, no es muy complicado. Pero lo improbable es que la criptografía sea el punto más débil. Hay tantas partes más inseguras en un sistema criptográfico... el software, el sistema operativo, la red, la gente... Siendo tan mala como puede ser la criptografía, y a menudo lo es, siempre hay algo peor.

H: A nivel gubernamental se utiliza la excusa de la seguridad para argumentar que es necesario un control y monitorización sobre las comunicaciones, por lo que existe un continuo debate con las organizaciones que abogan por la privacidad y el anonimato en Internet. ¿Realmente la seguridad exige la pérdida de la privacidad y el anonimato?

BS: Por supuesto que no. La próxima vez que alguien te diga que necesitas abandonar la privacidad para obtener seguridad, mírale a los ojos y dile: "cerrojo, alarma anticacos, valla alta". La mayor parte

de la seguridad no tiene nada que ver con la privacidad. Sólo la seguridad basada en identidad afecta a la privacidad, y hay limitaciones a esa aproximación.

H: ¿Alguna predicción en materia de seguridad informática? ¿Qué nos espera?

BS: Crimen. Crimen es lo antiguo y crimen es lo nuevo. Sólo cambian las tácticas, pero la motivación es atemporal.

H: ¿Qué sistema operativo y navegador utilizas?

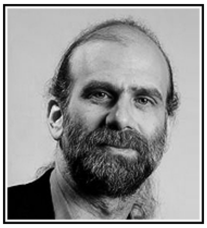
BS: Uso Windows, todavía XP, y Opera. Supongo que debería cambiar a Firefox, pero es que me gusta cómo funciona Opera.

H: Al margen de tu actividad profesional como Chief Security Technology Officer de BT, ¿a qué dedicas más tiempo últimamente? ¿Hobbies?

BS: Sigo escribiendo reseñas de restaurantes para una revista local y varios sitios online.

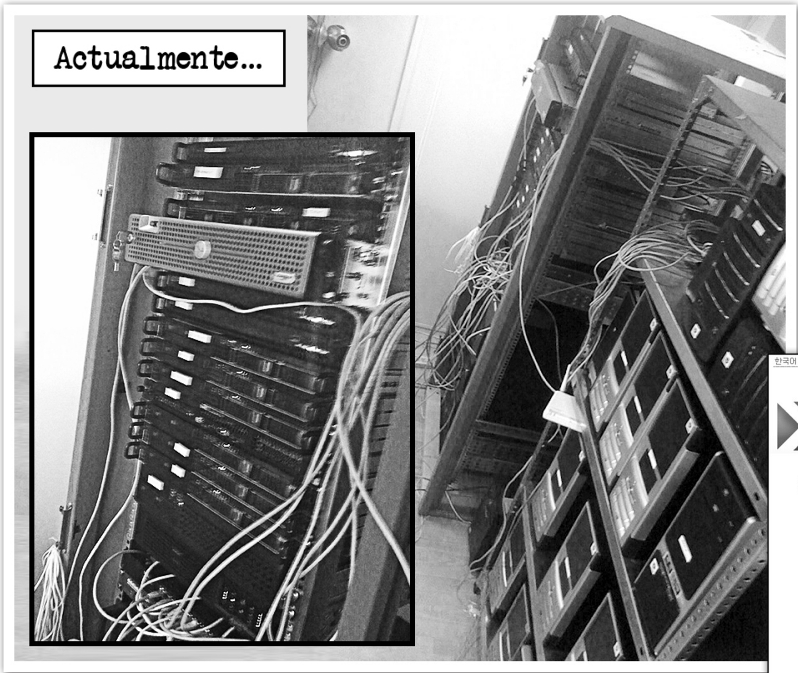
H: Un libro, una canción.

BS: El último CD de mi colección se llama "Better than the Real Thing," una compilación de cantantes de música folk irlandesa interpretando versiones acústicas de canciones de U2. El último libro que he leído es "Nudge," de Cass Sustein y Richard Thaler. Mi nuevo libro es "Schneier on Security." Acaba de salir, y parece un estupendo regalo para estas Navidades.




Primeros servidores de Hispasec y VirusTotal




Actualmente...


VIRUS TOTAL
Virustotal es un servicio de análisis de archivos sospechosos que permite detectar virus, gusanos, troyanos, y malware en general. Más información...
Análisis
Buscar Hashes
Estadísticas
Email/Uploader
Sobre VT
Seleccione un archivo
Nivel de Carga
Examinar...
Opciones de envío
Enviarlo sobre SSL
Enviar Archivo
Si deseas también puedes enviar usando tu cliente de correo electrónico.
VirusTotal © Hispasec Sistemas - Blog - Contacto: info@virustotal.com - Terms of Service & Privacy Policy

Capítulo

7

AÑO 2005

7D5

3725

11111010101



1104537600 – 1136073599

Durante este año...



_ El 5 de enero, desde el observatorio de Monte Palomar descubren el **nuevo planeta enano al que llaman Eris**, el más lejano del sistema solar.

_ El 11 de febrero, investigadores argentinos hallan en la Patagonia el único yacimiento existente hasta ahora de **huevos de dinosaurio** con embriones en su interior.

> El 16 de febrero entra en vigor el **Protocolo de Kioto**. Se trata del convenio mundial para el intento de reducción de gases y luchar contra el efecto invernadero. En 1997 los países industrializados se comprometieron en la ciudad de Kioto a ejecutar un conjunto de medidas para reducir los gases de efecto invernadero. Pactaron reducir en un 5% de media las emisiones contaminantes entre 2008 y 2012, tomando como referencia los niveles de 1990. El objetivo principal es disminuir el cambio climático de origen antropogénico cuya base es el efecto invernadero. Cada país debía reducir en distintos porcentajes sus emisiones. Mientras, el 1 de marzo de 2005, Madrid registra la temperatura más baja en un día de marzo de los últimos 105 años: -5°C en el Retiro, sufriendo uno de los inviernos más duros de su historia. Para muchos, el protocolo (que prometía un paso adelante) nació ya muerto en cuanto el gobierno de Estados Unidos (ni con Clinton ni con Bush al frente) no ratificó el acuerdo. En 2001 el gobierno de Bush se había retirado ya definitivamente del protocolo.

_ La noche del 12 de febrero **se incendia la torre Windsor de Madrid**. No se producen víctimas. Sus 106 metros de altura y 32 plantas estaban compuestos básicamente por oficinas. No se derrumbó hasta que es desmontada en agosto de ese mismo año y a finales del mismo mes, se abrirían a la circulación las calles adyacentes. Varias compañías con sede en el rascacielos lo pierden absolutamente todo. Se habla mucho de la seguridad física, de copias de seguridad y armarios ignífugos.

_ Durante principios del año 2005 el Gobierno español comienza a elaborar un nuevo Plan Técnico Nacional de la **Televisión Digital Terrestre** con la intención de impulsar esta tecnología en un mercado televisivo donde las emisoras de televisión digital por satélite (un panorama compuesto únicamente por Digital+, tras la fusión con su única competidora, Vía Digital) y las redes de cable copan el mercado de la televisión digital. El parque de receptores de TDT instalados se estima en ese año en unas decenas de miles, la mayoría de ellos los que distribuyó Quiero TV durante sus apenas dos años de existencia. De entre las medidas que contiene el nuevo plan destacan el adelanto del apagón analógico desde el año 2012 al 3 de abril de 2010. A partir de ese momento, todas las emisiones de televisión terrestres tendrán que realizase mediante técnicas digitales. También destaca la intención de aumentar el número de emisoras de TDT hasta el apagón analógico. Lenta pero segura, la TDT se popularizaría en 2007 gracias a los bajos precios de los decodificadores y a la integración en las nuevas televisiones.

_ En España, en el referéndum nacional para la ratificación de la **Constitución Europea** se aprueba la nueva Constitución con un 76,7% de los votos. La participación es de sólo el 42%. El 1 de junio en el

referéndum sobre la Constitución Europea celebrado en Países Bajos ganaría el "no" con un 60%.

_ El 2 de abril **muere Juan Pablo II** tras varias horas de agonía. Seis días después se realizan en Ciudad del Vaticano las exequias de Su Santidad Juan Pablo II, considerado el funeral más grande de toda la historia. El día 19 de de ese mes, Joseph Ratzinger es elegido Papa de la Iglesia Católica con el nombre de Benedicto XVI.

_ El 13 de junio **Michael Jackson** es absuelto de todos los cargos que se le imputaban.

_ Se publica **Debian GNU/Linux 3.1 "Sarge"**. Fruto de casi tres años de desarrollo continuo.

_ El 30 de junio se aprueba en España el **matrimonio entre personas del mismo sexo**.

_ A principios de julio se celebran nueve conciertos simultáneos en distintas ciudades del planeta **(Live 8)** para exigir el fin de la pobreza en el mundo.

_ El siete de julio se produce un múltiple **atentado terrorista en Londres**. Tres vagones de metro y un autobús urbano se ven afectados, causando 56 víctimas mortales y 700 heridos. Los atentados se relacionan con el apoyo del gobierno británico a la guerra de Iraq, en concreto con la foto de las Azores de 2003 en las que aparecían los líderes de los tres principales países que apoyaron la invasión. Un día antes la ciudad de Londres había sido designada por los miembros del COI como escenario de los Juegos Olímpicos del 2012.

_ A finales de agosto el **huracán Katrina** toca tierra estadounidense y produce uno de los mayores desastres que se recuerdan, con ciudades como Nueva Orleans completamente anegadas, junto con importantes pérdidas materiales y humanas en Luisiana, Mississippi, Alabama, Tennessee y el oeste de Florida. Se anuncian inicialmente más de 1.000 muertos. Las ayudas llegan tarde y mal. El presidente Bush es duramente criticado por su incapacidad de gestionar estos desastres en el, se supone, país más rico y preparado. Se popularizan en Internet las estafas relacionadas con la recolección de donativos para ayudar a los damnificados por el desastre.



_ A principios de diciembre se pone a la venta en España la consola **Xbox 360** de Microsoft. Es la primera consola que se lanza simultáneamente en Europa, Estados Unidos y Asia. Tiene una triple CPU a 3.2 Ghz y 512 MB de RAM.

_ Ricardo Galli compra a finales de 2005 el dominio **"Menéame"**, copiando la filosofía a Digg en España, pero con software libre. Se crearía a su alrededor una inmensa comunidad de fieles usuarios y clones. En noviembre de 2006 Martín Varsavsky, creador de Jazztel, Ya.com y FON, compraría el 10% (y más tarde el 33%) del portal.

_ El 31 de diciembre se añade de nuevo **un segundo al año** para compensar las diferencias entre la rotación de la Tierra y el tiempo atómico. Se hace a las 23:59:60.

Seguridad Informática

_ A comienzos de 2005 ya se rozaban las 20.000 muestras mensuales enviadas a **Virustotal.com**, en una escalada "sin control" que todavía hoy sigue experimentando.

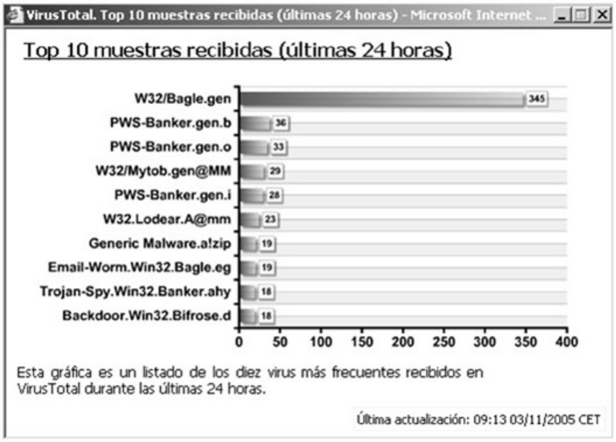
_ El **kernel de linux** comienza con mal pie el año. Se descubren varias vulnerabilidades que ponen sobre la mesa el descontento en los procedimientos actuales de parcheo y distribución de las versiones actualizadas del kernel. Se quejan de que, en algunos casos, esas correcciones no han estado disponibles en actualizaciones "oficiales" de los kernel hasta meses después. Esto es así porque la tendencia hasta ese momento fue el integrar esos parches en la versión en desarrollo de los kernel, cuya fecha de publicación puede estar a semanas o meses vista.

_ **Mytob** irrumpe. Se asiste a un goteo constante de nuevas variantes del gusano durante meses. La estrategia de su creador o creadores, sentando precedentes de la tendencia vírica actual, parece ser distribuir muchas variantes con pequeñas modificaciones para intentar evitar a los antivirus durante las primeras horas, mientras que se desarrolla la pertinente firma, y afectar al máximo número de usuarios.

_ A finales de febrero, se da a conocer que los contenidos del teléfono móvil de **Paris Hilton** han sido publicados en Internet. En un principio se baraja la posibilidad de que hubieran accedido a la tarjeta SIM, o de que se tratara de una intrusión a los servidores de T-Mobile aprovechando inyecciones SQL. Al final se hace público que el método empleado es mucho más sencillo, bastaba con contestar a la pregunta **"¿cuál es el nombre de su mascota favorita?"**. El teléfono de Paris, un Sidekick II de T-Mobile, permite mantener una copia de los contenidos en un servidor de Internet, accesible a través de la web. Como ocurre en muchos servicios en línea, T-Mobile utiliza el método de preguntas secretas para permitir el acceso a aquellos usuarios que han olvidado sus contraseñas. El nombre de su perro chihuahua era bien conocido a raíz de que la famosa heredera ofreciera en el pasado una recompensa de varios miles de dólares tras extraviarlo. El resultado es que a día de hoy cualquiera puede descargar todo el contenido del móvil de Paris Hilton. En él, se encontraban los teléfonos personales de Christina Aguilera, Avril Lavigne, Eminem, o Anna Kournikova... además de fotos personales (subidas de tono) realizadas con el móvil.

_ En marzo es liberado, para uso personal y educativo, el libro **"The Code Book"**. Escrito por Simon Singh, se trata de uno de los mejores libros de introducción a la criptografía.

En la mañana del 8 de marzo se da a conocer el fallo del juicio que enfrentaba a la empresa Tegam contra el científico francés **Guillaume T**. Finalmente Guillaume es condenado con una pena leve, inferior a la solicitada inicialmente por Tegam. El juez fija una condena condicional de 5.000 euros, que Guillaume no tendrá que pagar si no es condenado por otra causa durante los próximos dos años. En julio se sabe que Guillaume T. ha recurrido las dos sentencias condenatorias, la penal y la civil. Además se produce una novedad: una de las pruebas presentadas por Tegam contra Guillaume era que, junto a "otros", actuaba por intereses oscuros, acusándole en una carta dirigida el 7 marzo 2002 a la dirección del CNRS como un "terrorista informático conocido por el FBI y la DST". En esa carta también se acusaba directamente a otra persona, R.G., que también escribe con asiduidad en los foros de usenet. En un nuevo juicio de carácter civil, un Tribunal de Toulouse condena a Tegam por una falta por injurias cometida contra R.G. La historia no terminaría aquí.



_ A principios de 2005 se asiste de nuevo a una continua avalancha de variantes del gusano **Bagle**, que se propagaba a través de archivos adjuntos en mensajes de correo electrónico, enviados de forma masiva desde los sistemas infectados. Se publica **"Lessons from Virus Developers: The Beagle Worm History"**, estudio en el que se realiza un completo análisis de la evolución histórica del gusano, desde las primeras variantes detectadas a finales de enero de 2004 hasta las últimas, identificadas en enero de 2005. Presenta un análisis de las características más destacadas de las diversas variantes y la evolución en los mecanismos utilizados para su propagación y cómo poco a poco el gusano se iba haciendo más y más complejo, hasta el extremo de llegar a incorporar su propio servidor de nombres de dominio, la capacidad para desactivar o inhabilitar las medidas de seguridad instaladas en los sistemas infectados, la distribución en archivos cifrados con contraseña para saltarse los antivirus en el servidor de correo, etc... La intención es mostrar a Bagle como un ejemplo paradigmático de malware y una tendencia.

_ Durante una conferencia en Estados Unidos, tres investigadores del FBI demuestran cómo son capaces de **romper el cifrado WEP con clave de 128-bit de una red inalámbrica en tan sólo tres minutos**. El mecanismo tradicional de cifrado de las redes inalámbricas es WEP (Wired Equivalency Privacy), basado en el algoritmo RC4 utilizando claves de distinta longitud (entre 64 y 256 bits). Desde hace tiempo se conoce que WEP es, básicamente, un mecanismo inseguro al basarse en el uso de un secreto compartido entre el punto de acceso y las estaciones que acceden a la red. WEP no ofrece ningún mecanismo para la negociación de las claves utilizadas para el cifrado del tráfico. Es el momento de usar el estándar WPA (Wi- Fi Protected Access) que mejora las prestaciones de WEP mediante el intercambio de claves, aunque también permite una modalidad de secreto compartido. En 2004 se presentó la especificación 802.11i (también conocida como WPA2) que ofrece unos mecanismos fuertes de autenticación y cifrado del tráfico.

_ En mayo **Sober.q** causa una avalancha de spam con propaganda neonazi, enviadas desde máquinas zombi.

_ También en mayo, **Hispasec** lanza un servicio de alerta temprana en tiempo real a través de teléfonos móviles que, mediante mensajes de texto corto (SMS), avisará a los usuarios en caso de aparición de malware de especial incidencia o peligrosidad.

_ Un miembro del equipo de seguridad de FreeBSD detecta un **problema de seguridad en Hyper-Threading** implementado en los procesadores Intel Pentium Extreme Edition, Pentium 4, Mobile Pentium 4 e Intel Xeon. Un atacante podría obtener información sensible de la máquina atacada, incluyendo la posibilidad de robar una clave RSA privada que se esté usando en la máquina de la víctima. Hyper-Threading es un nuevo diseño de Intel que permite al software diseñado para múltiples hilos de ejecución (multi-threaded) procesar los hilos en paralelo dentro de cada procesador, lo que da como resultado un incremento en la utilización de los recursos de ejecución de los procesadores.

_ Las máquinas **zombi y botnets crecen desmesuradamente**. Nadie sabe a ciencia cierta el porcentaje exacto de máquinas de este tipo que están operando en la actualidad. Las máquinas zombi son

máquinas comprometidas al servicio de atacantes que las manejan desde un panel de control centralizado. Son usadas para robar sus datos y como plataforma para enviar correo basura. Las máquinas zombis se aglutinan en los denominados botnets, anglicismo que se refiere a la asociación en red (nets) de máquinas autónomas (bots, apócope del término sajón robots). Todavía durante 2006 y 2007 crecerían incluso más.

_ Se detiene a 18 personas en Israel, entre las cuales destacan altos ejecutivos de tres grandes corporaciones, por **espionaje industrial a través de troyanos**. Durante la investigación se encuentran en posesión de los acusados documentos e imágenes de la competencia y terceras empresas de un enorme valor comercial. Estiman que el espionaje se llevó a cabo durante más de un año.

Aparece **PGPcoder**, el troyano chantajista. Cifra los archivos de los sistemas y solicita dinero a los usuarios afectados si quieren volver a restaurarlos. La realidad es que, debido a un mal diseño de su creador, el troyano utiliza un algoritmo de cifrado muy simple, basado en valores fijos, que permite invertirlo y recuperar automáticamente los archivos. Cuando se ejecuta en un sistema, cifra todos los archivos que localiza con las extensiones .xls, .doc, .txt, .rtf, .zip, .rar, .dbf, .htm, .html, .jpg, .db, .db1, .db2, .asc y .pgp. Creando además unos archivos de texto, "ATTENTION!!!.txt", con el siguiente mensaje:

Some files are coded.
To buy decoder mail: n781567@yahoo.com
with subject: PGPcoder 000000000032

En definitiva, que si el usuario infectado quiere volver a acceder a sus documentos, hojas de cálculo, fotografías, etc., debe "comprar" el descodificador que supuestamente el autor le enviaría por correo.

A pesar del nombre usado (PGPcoder) para denominar al malware, el autor del troyano programó un algoritmo de cifrado bastante simple sin clave externa, lo que permite invertir el algoritmo para recuperar los archivos sin tener que pasar por el chantaje. Hispasec obsequia con una camiseta a los tres primeros lectores que envían un script o programa (incluyendo fuentes) que debería descifrar otro archivo cifrado por el troyano PGPcoder.

_ Debasis Mohanty, un investigador hindú, rompe el sistema de protección **Windows Genuine Advantage (WGA)** de Microsoft. Desarrolla una herramienta denominada genuinecheck.exe con la que se permite descargar software hasta ahora reservado a las copias que el servidor de Microsoft considerase legales.

_ En una noticia aparecida en el New York Times, se afirma que **Microsoft está en conversaciones con Claria, más conocida anteriormente como Gator**, una de las principales productoras de adware. Choca directamente con los nuevos intereses de Microsoft centrados en productos antivirus y antispyware. A raíz de esta noticia se disparan los rumores. ¿Detectará el motor antispyware de Microsoft un producto que es suyo? Las últimas actualizaciones de Microsoft AntiSpyware detectan el adware de Claria instalado en el sistema pero, por defecto, recomienda la acción de ignorarlo, es decir, no eliminarlo del sistema, mientras que otras soluciones gratuitas como SpyBot, además de detectar el adware de Claria lo elimina por defecto.

_ **Halvar Flake**, especialista en ingeniería inversa y responsable de la consultora Sabre Security, decide investigar sobre el parche crítico MS05-025 publicado para Microsoft Internet Explorer, centrándose en la vulnerabilidad en la gestión de documentos gráficos portables PNG que permite la ejecución de código. Utilizando herramientas propias y comparando las versiones parcheadas y sin parchear, Flake localiza los cambios específicos que introduce el parche MS05-025 en menos de 20 minutos. Flake documenta cómo los parches rápidos y teóricamente inocuos pueden ser fuente de obtención de código vulnerable. Esta teoría sería de nuevo retomada años después. Se llegaría a barajar la posibilidad de crear una forma automatizada de programar exploits a partir de parches recién publicados.



Se publica en agosto el número 63 de la **la revista online Phrack**, con el que esta publicación online y gratuita se despide. Es el fin de la primera publicación que se distribuyó exclusivamente de forma electrónica. Con casi veinte años de historia, la revista Phrack es todo un referente y una de las publicaciones más prestigiosas en el mundo de la seguridad informática. En su larga trayectoria, en Phrack se han publicado las primeras referencias a numerosas técnicas como, por ejemplo, el artículo de Aleph One "Smashing the stack for Fun and Profit" donde se desarrollaban las técnicas de ejecución de código en la pila inyectado a través de desbordamiento de memoria intermedia. Otro artículo histórico describía el funcionamiento del número de emergencias (911) de los Estados Unidos. La publicación de este artículo originó una serie de demandas judiciales y el encarcelamiento de los editores, acusados de publicar material confidencial robado de la compañía telefónica Bell South y que ponía en peligro la seguridad de los ciudadanos norteamericanos. Durante el juicio, por el que se pedían una indemnización de 80.000 dólares se demostró que esa información estaba al alcance de cualquier persona por sólo 13 dólares.

Inicialmente la revista Phrack se centraba en la seguridad de las redes de comunicaciones, documentando un gran número de vulnerabilidades y falsas medidas de seguridad implementadas por las compañías telefónicas. Con el tiempo, su contenido fue moviéndose hacia el mundo de los ordenadores y la seguridad informática. Algunos nombres míticos en la historia de la seguridad informática guardan una relación muy directa con la revista Phrack. Desde los editores originales, Taran King y Knight Lightning, hasta grupos como Legion of Doom.

La conmemoración de este último número se realiza a través de la publicación de una edición especial en papel (por tercera vez en la historia), que se reparte durante la celebración del "What the Hack" y Defcon 13.

_ Aparecen una serie de variantes de malware capaces de aprovechar la vulnerabilidad (remota y que permite la ejecución de código) parcheada en el boletín MS05-039 de Microsoft, que afecta a Windows 2000. **Zotob** y otras variantes comienzan a causar estragos. Medios como la CNN, ABC y The New York Times se ven azotados por este gusano. Como efecto colateral los sistemas infectados se reinician constantemente, lo que impide trabajar con ellos.

_ El 1 de agosto se pone en marcha el **blog del laboratorio de Hipsasec**. Nace como un espacio más directo e informal donde se tratará cualquier tema a título personal. Apuntes técnicos, anotaciones,

opinión, notas de humor y, en definitiva, cualquier tipo de contenido que por alguna extraña razón nos haya resultado interesante, sin que exista una periodicidad o temática prefijada.

_ En la edición de la Black Hat estaba programada una presentación por parte de Michael Lynn sobre cómo **comprometer los routers Cisco**. En un intento de censurar dicha información, Cisco recurre a tácticas legales para impedir la divulgación de la información. El efecto es el contrario al buscado: hay presentación, la documentación cuelga de numerosos sitios de Internet, y el caso despierta un gran interés tanto en investigadores de seguridad como en los medios de comunicación. En la reunión Def Con posterior se observan grupos de trabajo discutiendo sobre cómo reproducir de forma práctica el estudio de Lynn (que no aportó detalles técnicos). Cisco publica un parche dos días después de la charla.

Un australiano consigue anular una multa de tráfico ante la imposibilidad de las autoridades de tráfico de **demostrar fehacientemente que la imagen registrada por un radar no ha sido alterada**. El australiano circulaba con su coche por una carretera que estaba siendo controlada con un radar. El abogado que representa al amonestado recurre la denuncia, argumentando que no se ha probado que la imagen obtenida por la cámara asociada al radar no ha sido modificada de ninguna forma. Las autoridades australianas del tráfico responden a esta argumentación que se utiliza el algoritmo matemático MD5 para obtener una suma de control de las imágenes obtenidas por el radar. El problema radica en que no encuentran a ningún perito que demuestre ante el tribunal la validez de dicho algoritmo. La función de hash criptográfico MD5 (Message-Digest algorithm 5) lleva ya años mostrando signos de debilidad, inadecuado para los tiempos que corren. Si bien se ha llevado varios varapalos desde su creación, a principios de 2008 se demostraría que es posible crear arbitrariamente dos flujos de datos que resulten en el mismo hash o firma. Marc Stevens, Arjen Lenstra, y Benne de Weger harían público un método por el que, añadiendo un puñado de bytes a un archivo, se podría hacer que su firma, su hash MD5, fuese idéntico a otro fichero arbitrario. La diferencia en este caso es que las colisiones pueden ser elegidas, provocadas sobre dos ficheros cualesquiera. Lo conseguirían con una sola máquina en menos de dos días. Un tiempo más que razonable.

_ En un estudio divulgado por la asociación norteamericana de ingenieros IEEE-USA, en su publicación Today's Engineer, con título **"United States Facing Cyber Security Crisis"**, se afirma que la infraestructura de seguridad y tecnologías de la información en EEUU es altamente vulnerable ante ataques terroristas y criminales. Las instalaciones afectadas y comprendidas en el estudio van desde los sistemas de control de tráfico aéreo, redes de electrificación y suministro energético, sistemas financieros, además de redes de inteligencia y militares. Cliff Lau, perteneciente al comité de política de I+D de IEEE-USA, explica que de seguir las cosas como están, las perspectivas a cinco años vista son realmente inquietantes. Lau define la situación como "al borde de la pérdida de control", una vez analizada la situación actual y las perspectivas esperadas para ese período.

_ En agosto el FBI anuncia la detención en Marruecos de Farid Essebar, alias "Diablo", de 18 años de edad, y de su supuesto cómplice en Turquía Atilla Ekici, alias "Coder", de 21 años. Ambos son los **sospechosos de distribuir los gusanos Zotob y Mytob**. Según la investigación sus prácticas tenían un móvil económico relacionado con el fraude a usuarios de entidades financieras. Los dos detenidos se conocían únicamente por Internet. Microsoft juega un papel importante en su localización, al ofrecer pistas importantes que encontraron al analizar el código de los gusanos. El código original de Zotob incluye el texto "Botzor2005 Made By .... Greetz to good friend Coder. Based On HellBot3", y además el

gusano intenta conectar por el puerto 8080 a un servidor IRC en la dirección "diablo.turkcoders.net". Ambas pistas, fruto de un exceso de confianza o ansias de protagonismo son claves para el inicio de la investigación.



El debate Firefox (que no saca su versión estable 1.5 hasta noviembre de 2005) vs. Internet Explorer está en su mayor auge. Firefox ya alcanza el 7% de uso, y llegaría al 9 a principios de 2006. Se convierte en una amenaza para Internet Explorer que, tras haber conseguido picos del 95% de uso en 2004, se mueve en esos momentos en el 87%. Para poder seguir en el juego, Opera se ve obligado a volverse completamente gratuito en noviembre, eliminando la publicidad que incluía en su navegador para los que lo descargaran sin pagar. Un estudio de Symantec suscita el **debate sobre qué navegador es más seguro.** El titular que trasciende del informe es que Firefox ha tenido más vulnerabilidades que Internet Explorer en lo que ha transcurrido de año. Aunque el dato es cierto, se puede argumentar que aún así es más seguro navegar con Firefox que con Internet Explorer, puesto que el malware siempre intenta aprovechar los sistemas de uso mayoritario. El que los atacantes decidan fijar su atención más en Internet Explorer que en Firefox poco tiene que ver con la facilidad de explotación en aplicaciones de código abierto o cerrado. En junio de 2008 se detectaría en nuestro laboratorio de Hispasec un ejemplar de malware no interesado en la amplia base de usuarios de Internet Explorer y exclusivamente dirigido a los de Firefox.

En el informe de Symantec se afirma que el tiempo medio entre que se publica una vulnerabilidad y aparece el exploit ha descendido a 6 días, mientras que sitúa la media en 54 días el tiempo que transcurre entre la aparición de una vulnerabilidad y la publicación del parche. Esto abre una ventana de 48 días donde los sistemas pueden ser vulnerables.

_ En septiembre Creative lanza alguna remesa de sus reproductores Neeon con un "extra" en la memoria: un ejemplar del gusano **Wullik-B**.

_ **Nessus** anuncia que abandonará la licencia GPL para su próxima versión (la 3), mientras que la empresa Sourcefire, los padres de **Snort**, son comprados por Check Point. Nessus nació de la mano de Renaud Deraison, quien creó en 2002 la empresa Tenable Security. Mientras que Martin Roesh, el creador de Snort, fundó la empresa Sourcefire en el 2001. Ante las nuevas noticias, Martin Roesh da las gracias a la comunidad open source, y asegura la continuidad del proyecto Snort en las mismas condiciones, cosa que cumpliría. Renaud Deraison afirma que Nessus 2 seguirá bajo GPL aunque se limitará a parchear los problemas que puedan encontrarse, mientras que Nessus 3 con importantes mejoras será gratuito pero no se distribuirá bajo GPL.

_ Comienzan a popularizarse las **tarjetas de coordenadas** entre las entidades bancarias para luchar contra el phishing. La idea es que en cada operación que implique movimiento de dinero, se pida una clave de entre un buen número de coordenadas disponibles en una tarjeta. Si un usuario realiza una operación, sólo introduce una o dos coordenadas y, aunque sean robadas, la posibilidad de que se soliciten las mismas en una operación posterior son mínimas. El phishing evoluciona y se detecta un caso contra eBankinter en el que después de introducir el usuario y contraseña se presenta un formulario donde se deben introducir todos los números de la tarjeta de coordenadas. Así el atacante está seguro de disponer de todas las posibilidades. Anteriormente se había observado un caso contra LaCaixa en el que se pedía

directamente el envío de la tarjeta completa por fax. Los usuarios pican, pensando que supone una mejora de la seguridad. Sería una técnica habitual y exitosa que aún se mantiene en la actualidad.

Sony utiliza un rootkit. La técnica utilizada por el software anticopia distribuido en algunos CDs de Sony BMG es similar a la empleada por malware avanzado para evitar ser descubiertos por los antivirus. El problema se agrava porque la instalación de ese software, que se lleva a cabo sin informar previamente al usuario que compra y utiliza legalmente el CD, abre en Windows una brecha de seguridad que pueden aprovechar virus, gusanos y troyanos. Ante la avalancha de críticas, Sony BMG insiste en que su software no es malicioso ni compromete la seguridad de sus clientes, sin embargo reconoce que puede plantear vulnerabilidades potenciales y se ve forzada a ofrecer una utilidad ActiveX para desinstalarlo. En noviembre aparece el primer troyano que utliza el rootkit de Sony para esconderse. Aprovecha una de las funciones del rootkit de Sony que oculta por defecto todas las entradas del registro, procesos, carpetas y archivos cuyo nombre comiencen por "sys". Un análisis en el laboratorio de Hispasec descubre que el troyano se equivoca al introducir una clave en el registro que le permita ejecutarse en cada inicio, perdiendo efectividad. Poco después, tras incluso detectarse una vulnerabilidad en el propio ActiveX necesario para la desinstalación del programa anticopia (que volvía vulnerable a los sistemas que lo habían instalado) la situación se vuelve insostenible y Sony abandona definitivamente el rootkit anticopia.



_ Se detecta **Lupper/Lupii**, malware diseñado para sistemas Linux. El troyano aprovecha la vulnerabilidad XML-RPC detectada en julio de 2005, en servidores de PHP en máquinas Linux.

_ **Zero Day Initiative** de TippingPoint publica su primera alerta en octubre. Se trata de una compañía, filial de 3Com, que paga a investigadores por sus vulnerabilidades descubiertas, a cambio de cedérselas en exclusiva. TippingPoint se asegura así de una revelación responsable y, además, protege a los clientes de sus productos en primicia ante la vulnerabilidad descubierta. Sería una iniciativa con bastante éxito que motivaría la investigación entre los analistas de seguridad. Un poco más tarde, en febrero de 2006, iDefense ofrecería hasta 10.000 dólares por vulnerabilidades que permitiesen ejecución de código en Windows. TippingPoint contraatacaría ofreciendo hasta 50.000.

_ Se detecta un desbordamiento de memoria intermedia en la versión 2.0 del firmware de la **PSP (Play Station Portable)** que permite la ejecución de código. Aprovechando esta vulnerabilidad se publica una utilidad que permite realizar una regresión a la versión 1.5 del firmware, con la ventaja de que con ella el usuario puede ejecutar software "no autorizado" por Sony. También se crea un troyano que, disfrazado de utilidad para bajar de la versión 2.0 a la 1.5 del firmware, en realidad elimina varios archivos críticos de la flash de la PSP.

_ El año acaba con la **vulnerabilidad en tratamiento de archivos WMF de Windows** en todo su apogeo. Se detecta que se está usando un exploit que aprovecha una vulnerabilidad de Microsoft para la que no existe parche, y que puede ser explotada por atacantes remotos para ejecutar código. Si la víctima utiliza Internet Explorer, puede provocarse la ejecución automática de código arbitrario al visitar una web especialmente manipulada. 2006 empezaría con esta vulnerabilidad, y todo lo que dio de sí, en numerosos titulares.

01/02/2005 Publicidad falsa de Terra en relación a su antivirus

"Antivirus detecta y bloquea todos los virus desconocidos y asegura la protección contra las variantes que se crean a partir del virus original". Con esta frase lapidaria, publicada en su web, Terra vende el servicio de antivirus basado en el motor de McAfee.

A estas alturas sobra decir que no existe ninguna solución que pueda garantizar un 100% de seguridad. En el caso de los antivirus es algo totalmente obvio, por definición no pueden detectar todos los virus desconocidos o de nueva creación, y de hecho cualquier solución antivirus también pierde un porcentaje de virus que están pululando por Internet y cuyas muestras aun no han analizado en sus laboratorios e incorporado a sus actualizaciones.

En la misma web podemos leer "Contrate Antivirus ahora y olvídese de los virus. Antivirus comprueba automáticamente si hay nuevas versiones o actualizaciones de virus para que su protección esté siempre actualizada". Ya es contradictorio que un motor que dice detectar todos los virus desconocidos necesite actualizaciones de virus.

Anuncios como el de Terra, además de ser publicidad falsa (con lo que ello pudiera conllevar), son claramente contraproducentes para los usuarios, ya que crean una falsa sensación de seguridad. Los usuarios deben ser en todo momento conscientes de las limitaciones intrínsecas de las soluciones antivirus, y en ningún momento deben olvidarse de los virus, o terminarán infectándose.

Los antivirus son una capa de seguridad recomendable y necesaria en sistemas domésticos y entornos corporativos, pero como toda solución tiene sus limitaciones, y es entonces cuando la única línea de defensa es el factor humano. Si vamos promulgando que el antivirus es infalible, que el usuario debe olvidarse de los virus por completo, o incluyendo un pie en el correo electrónico diciendo que el mensaje está libre de virus... al final lograremos que, por un exceso de confianza, el usuario se infecte.

Sin ánimo de cargar las tintas contra McAfee, que suponemos habrá sido víctima del marketing de Terra, algunos datos para corroborar lo obvio:

En VirusTotal recibimos durante el mes de enero 18.234 muestras de usuarios de Internet, de las cuales 10.297 fueron detectadas como infectadas (uno o más antivirus la identificaron como virus o malware). De esas 10.297 muestras infectadas, McAfee sólo detectó 4.062, es decir, un 39,45% de acierto. Si hiciéramos un ranking basado en el porcentaje de detección, McAfee ocuparía el 7º puesto.

Seguramente a más de uno le sorprenderá un porcentaje de detección tan bajo. Hay que decir en defensa de McAfee que las muestras que suelen enviar los usuarios a VirusTotal son bastante heterogéneas, no sólo se envía el típico gusano de turno. Pero, al fin y al cabo, son muestras infectadas enviadas por los usuarios y que circulan por Internet.

En el siguiente enlace podemos observar una captura de la publicidad de Terra, que esperamos sea corregida a la mayor brevedad:
http://www.hispasec.com/images/mcafee_terra_20050201.png

Bernardo Quintero

12/04/2005 Fuerza bruta contra creatividad, los gusanos buscan el dinero

En los últimos días estamos asistiendo a un goteo constante de nuevas variantes del gusano Mytob. La estrategia de su creador o creadores, a falta de nuevas ideas en la propagación de gusanos, parece ser distribuir muchas variantes con pequeñas modificaciones para intentar evitar a los antivirus durante las primeras horas, mientras que se desarrolla la pertinente firma, y afectar al máximo número de usuarios.

Pese al bombardeo continuo, hay días que hemos contado hasta 5 nuevas variantes, la propagación hasta el momento es discreta, no protagonizando ningún pico especialmente relevante de infecciones. No obstante está por ver si esta estrategia está dando realmente sus frutos y si, sin necesidad de una propagación relámpago, poco a poco está logrando un parque importante de sistemas infectados.

Las motivaciones por las que se crea un gusano pueden ser de lo más variadas, pero en este caso apunta a que el interés se centra en controlar el mayor número de sistemas de forma remota, probablemente para realizar ataques distribuidos, desde envío de spam, hasta una denegación de servicios, pasando por el robo de credenciales de acceso a sistemas bancarios.

Y es que en los últimos tiempos se ha perdido el "romanticismo" en la creación de virus y gusanos, si es que alguna vez pudo describirse en esos términos, especialmente cuando, en el mejor de los casos, terminan causando auténticos quebraderos de cabeza, sin contar destrozos mayores.

Hoy día, hemos pasado de los experimentos de estudiantes a la mafia organizada, a auténticos profesionales del malware que, por encima de todo, buscan un rendimiento económico.

En un primer momento pudiera parecer que esta profesionalización, con mayores recursos a sus espaldas, se traduciría en unos especímenes más sofisticados. Sin embargo podemos observar que más bien es al contrario, se ha pasado de la creatividad a la fuerza bruta. Cada vez hay más proliferación de malware, pero se ha perdido en "calidad" técnica.

Mientras para los creadores de virus de la vieja escuela parte de la motivación venía dada por inventar y experimentar con nuevas técnicas, hoy día la mayoría lo que busca son resultados cuantitativos. Y todo parece indicar que resulta más rentable en esos términos dedicarse a modificar continuamente el código del mismo gusano más que a buscar nuevos enfoques que tal vez no tengan una rentabilidad directa en número de infecciones.

En el caso de la avalancha actual de variantes de Mytob, por ejemplo, podemos ver como se utiliza la típica estrategia del envío del archivo infectado adjunto por e-mail junto a otras técnicas bien conocidas, como es aprovechar la vulnerabilidad LSSAS que Microsoft parcheó el año pasado, la misma que explotó el famoso gusano Sasser.

Y con esa estrategia bien conocida y para las que existen formas básicas de prevención, ¿logran infectar sistemas?. Afirmativo. Internet es enorme, y si bien mucha gente, como nuestros lectores, cumplen unas normas básicas de seguridad que les permite prevenir este tipo de gusanos, existe un gran número de sistemas y usuarios sin protección alguna, a los que un gusano de e-mail les debe sonar a algo parecido a un insecto.

Es para este parque de máquinas y usuarios desprotegidos para los que se desarrolla este tipo de gusanos y otro tipo de malware que a nosotros nos molesta más por el spam que pueden llegar a generar que por el peligro de infectarnos.

Es tal la lucha de los creadores de este tipo de malware por controlar ese parque de máquinas desprotegidas que es habitual ver guerras entre ellos, por ejemplo que una determinada familia de gusanos desactive a otros gusanos en la competición por hacerse con los sistemas más débiles.

En definitiva, tal y como están las cosas, no nos queda más remedio que sufrir la avalancha cotidiana de nuevas variantes y versiones con las mismas técnicas más o menos reconocidas.

No obstante, nunca debemos bajar la guardia, cada cierto tiempo, al menos ha sido así durante los últimos años, siempre ha surgido algún nuevo espécimen especialmente virulento, y últimamente las aguas están muy calmadas...

Bernardo Quintero

21/04/2005 Virus y móviles, una tendencia al alza

Aunque aun son testimoniales, el número de nuevos virus, troyanos y gusanos para dispositivos móviles va en claro aumento. De momento no dejan de ser pruebas de concepto, con un poder de propagación limitado, pero es un indicador claro de que estamos viviendo los inicios de una nueva etapa/plataforma para el malware.

Lo que comenzó como una anécdota a mediados del pasado año, con la aparición de Cabir, un gusano para Symbian que se propagaba a través de Bluetooth, empieza a ser ya una constante este año con la aparición de un nuevo espécimen o variantes prácticamente todos los meses. En cualquier caso aun siguen siendo básicamente muestras de laboratorio, con escasa incidencia en el mundo real, y con una producción ínfima en comparación con la aparición de malware para PCs.

Básicamente, hasta la fecha, la mayoría del malware destinado a móviles se ha desarrollado para Symbian, no en vano es la plataforma dominante con más del 90% del mercado, con Nokia como principal “culpable” de ese dominio.

En cuanto a la tipología del malware, a principios de año apareció Lasco, un virus capaz de infectar a otros ejecutables SIS del dispositivo. El resto se puede dividir en dos grandes grupos, por un lado tenemos a los troyanos que se hacen pasar por aplicaciones legítimas y que incluyen algún código malicioso, normalmente desactivando alguna de las funcionalidades de los móviles, y por otro lado a los gusanos que intentan propagarse a través de Bluetooth.

La propia tecnología Bluetooth ya supone una traba para las propagaciones masivas, debido a que el alcance de la conexión inalámbrica no supera los 10 metros. Es como si un gusano infectara un PC en la oficina y sólo pudiera afectar a otros ordenadores que estén a la escucha en un radio de 10 metros.

Si bien en el caso de los móviles ayuda el hecho de que no permanecen fijos en una ubicación, sino que se trasladan con su dueño, este tipo de estrategia queda lejos de la potencia de propagación que tiene un gusano típico de Internet. Por ejemplo, a través del e-mail, puede llegar a un parque potencial de millones de máquinas en cuestión de minutos.

Sin embargo el pasado mes de marzo ya tuvimos un toque de atención con la aparición de Comwar, un gusano que, además de propagarse por Bluetooth, se enviaba a toda la lista de contactos del móvil infectado

a través de mensajes multimedia (MMS), con una estrategia muy similar a la de los típicos gusanos de Internet por e-mail.

Afortunadamente el incidente no pasó a mayores, pero todos los indicios apuntan a que la cuenta atrás ha comenzado en este nuevo campo de batalla, y que la amenaza de una infección masiva empieza a contemplarse como una posibilidad a medio plazo.

Bernardo Quintero

26/05/2005 Nueva generación de phishing rompe todos los esquemas

Hispasec demuestra como es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco.

Hasta la fecha las recomendaciones para acceder de forma segura a la banca electrónica hacían hincapié en comprobar que la URL del navegador comenzara por https:// seguido del nombre de la entidad, así como que haciendo doble click en el candado que aparece en la parte inferior del navegador se comprobara el certificado, para cerciorarse de que el usuario estaba navegando en el servidor seguro de la entidad.

En un estudio sobre phishing avanzado, llevado a cabo por Hispasec de cara a prevenir futuras técnicas de ataque, se han detectado varias áreas de oportunidad, una de ellas hace inútiles las recomendaciones anteriores.

Básicamente se trata de aprovechar un tipo de vulnerabilidad muy común en aplicaciones webs, como es el Cross-Site Scripting (XSS), para modificar el contenido de la web que el usuario visualiza en su navegador. Este tipo de vulnerabilidad es bien conocida en el mundo de la seguridad, si bien en contadas ocasiones se considera de un riesgo medio y no se le presta la atención que se merece.

En el análisis realizado por Hispasec en webs reales de entidades bancarias se demuestra como es posible aprovechar este tipo de vulnerabilidad para llevar a cabo ataques de phishing avanzados. Este tipo de ataque permite al usuario comprobar el certificado de seguridad del web de la entidad que está visitando sin que pueda observar nada irregular, hasta la fecha uno de los métodos más seguros que el usuario tenía para cerciorarse de que no estaba siendo víctima de un phishing y que sus datos se transmitían de forma cifrada a la entidad bancaria.

Para hacer más visual y comprensible el alcance del problema, Hispasec ha preparado tres vídeos (flash) donde se detalla un caso real de phishing sobre una entidad realizado como prueba de concepto (avisado y corregido antes de publicar estas líneas). El primero de los vídeos muestra la perspectiva de la víctima que sufre la estafa, el segundo como el atacante ha preparado el phishing, y un tercero genérico explicando de forma gráfica las implicaciones de los Cross-Site Scripting en los servidores seguros.

Recomendamos encarecidamente la visualización de los vídeos flash disponibles en la dirección:

http://www.hispasec.com/directorio/laboratorio/phishing/demo

De manera independiente a si es un problema de implementación o vacío en las especificaciones, parece también oportuno que los navegadores, al igual que avisan cuando desde una conexión segura se van a visualizar elementos no seguro, incorporaran un mecanismo para alertar cuando se están cruzando contenidos de diferentes servidores seguros. De lo contrario siempre rondará la duda en el esquema de autenticación de servidores web seguros.

Además de las implicaciones técnicas y de la dificultad que entrañaría a los usuarios detectar este nuevo tipo de phishing, el ataque sitúa gran parte de la responsabilidad en manos de la entidad bancaria afectada, ya que es posible llevarlo a cabo aprovechando vulnerabilidades en la programación de su web, y no se facilitan al usuario mecanismos adicionales para poder prevenir y detectar el fraude de forma sencilla.

Hispasec ha llevado a cabo un estudio preliminar sobre 50 sitios webs de entidades bancarias españolas, realizando un análisis superficial de la portada, detectando que 6 de ellas (12%) presentaban vulnerabilidades del tipo Cross-Site Scripting (XSS) evidentes en su primera página.

Debemos hacer hincapié en que las vulnerabilidades XSS pueden estar presentes en cualquier página de la entidad, no sólo en la portada, por lo que el número real de entidades afectadas puede ser muy superior.

Dada las implicaciones en materia de seguridad que puede tener este tipo de debilidades para sus clientes, Hispasec recomienda encarecidamente a todas las entidades bancarias realicen periódicamente auditorias de sus servicios webs incluyendo, de forma especial, el análisis por parte de expertos del diseño y programación de sus páginas.

Por su parte los usuarios deberán evitar a toda costa utilizar enlaces que les lleguen a través del correo electrónico o mediante otra vía para enlazar con servicios sensibles, como es el caso de la banca electrónica. Para evitar en concreto este nuevo tipo de ataque se recomienda que los usuarios escriban de forma manual y directa la dirección web de su banco en el navegador.

Hispasec ha notificado los detalles de las vulnerabilidades detectadas a las entidades bancarias que forman parte del grupo de cooperación anti-phishing recientemente formado, y de forma especial a las entidades afectadas, de manera independiente a su participación en el grupo, para que puedan proceder a su pronta corrección y prevenir este tipo de ataques.

Por ultimo destacar el interés y eficiencia de las entidades afectadas en la corrección de los casos detectados, de forma especial queremos agradecer a Bankpyme por su diligencia ejemplar a la hora de abordar y solucionar el problema.

Bernardo Quintero

27/07/2005 Troyanos y phishing, una amenaza en alza

Los phishers incorporan masivamente el uso de troyanos especializados en la captura de credenciales como complemento a las técnicas habituales de fraude, basadas en la falsificación de páginas web y formularios de entidades bancarias.

Que el número de ataques phishing no deja de aumentar es un hecho evidente, así lo reflejan tanto las estadísticas que recopilan este tipo de incidentes como los casos concretos que cualquiera de nosotros podemos llegar a recibir en nuestro buzón de correo.

Existe además una amenaza íntimamente relacionada con el phishing tradicional, los troyanos especializados en el robo de las credenciales de acceso a servicios de entidades bancarias.

El fin de estos troyanos y el daño que causan al usuario es el mismo que cualquier phishing basado en el engaño mediante mensajes y páginas falsas. Con el agravante de que el troyano puede permanecer en el sistema del usuario semanas o meses capturando y enviando a los phishers todas las credenciales de acceso utilizadas durante ese tiempo, sin que el usuario pueda percatarse a simple vista de lo que ocurre.

La realidad es que, en la actualidad, el número de incidentes relacionados con la suplantación de identidades en los servicios de banca electrónica tiene su principal origen en este tipo de troyanos, más que en el phishing más tradicional y reconocido basado en el engaño mediante mensajes y páginas webs que imitan las de la entidad legítima.

En los últimos casos de phishing analizados por Hispasec, y en los que hemos logrado el acceso a los datos obtenidos por los phishers, se comprueba que cuantitativa y cualitativamente los troyanos son más efectivos para los intereses de los atacantes, en comparación con los datos obtenidos mediante la imitación de los formularios de acceso a banca electrónica.

Por su naturaleza, los troyanos plantean más problemas de prevención a las propias entidades bancarias. Ya que a diferencia del phishing tradicional no es un ataque contado en el tiempo, con un principio (cuando se detecta el envío del spam con el mensaje falso) y un fin (cuando se logra desactivar la página fraudulenta), y por tanto no pueden establecer las medidas de vigilancia especial que ponen en marcha en estos casos.

Además los troyanos bancarios pueden tener un campo de acción muy amplio. Mientras que un phishing tradicional se diseña contra una entidad en concreto, el troyano permite diseñarlo para que actúe capturando las credenciales de un gran número de entidades. De hecho, a día de hoy se están capturando credenciales de usuarios cuyas entidades no han sufrido ataques de phishing tradicional.

Dada las ventajas que los troyanos suponen para los phishers, no es de extrañar que la corriente actual de este tipo de ataques combine ambas técnicas, de modo que los ataques de phishing que simulan las páginas webs de servicio de banca electrónica incluyen además la instalación de troyanos para capturar las credenciales de acceso.

Un ejemplo de como funcionan este tipo de ataques combinados lo podemos encontrar en el último caso de phishing contra clientes del BBVA.

Desde el punto de vista del usuario, recibe en su buzón de correo electrónico un mensaje supuestamente emitido por el BBVA, con dirección de remite bbva-supporte.es y la imagen corporativa de la identidad (logotipos, etc.), donde se le informa que debe rellenar un formulario para validar su identidad o de lo contrario su cuenta será bloqueada.

El formulario incluye el número de usuario, clave de acceso, clave de operaciones, PIN de la tarjeta, código de verificación de la tarjeta y documento de identidad.

Si el usuario, víctima del engaño, introduce sus datos en el formulario, éstos serán enviados a los phishers, que desde ese momento podrán suplantar la identidad del usuario para acceder y realizar operaciones a través de la banca electrónica en su nombre.

Cuando el usuario pulsa el botón de aceptar del formulario, además de proceder al envío de los datos

introducidos (aunque éstos sean falsos), se le redirige a una página web que incluye diversos scripts que tienen como fin explotar algunas vulnerabilidades de Internet Explorer para instalar un troyano.

Si el usuario no cuenta con una versión actualizada de Internet Explorer o una solución antivirus que detecte los scripts maliciosos o el troyano, el ejecutable preparado por los phishers se descargará e instalará en su sistema. A partir de entonces todas las credenciales que utilice en sus accesos, bien al BBVA u a otros servicios por Internet, pueden ser capturadas y enviadas a los phishers.

En el momento de escribir estas líneas el phishing del BBVA sigue activo, por lo que evitaremos dar detalles de las direcciones para evitar cualquier infección accidental.

La respuesta de las soluciones antivirus a las diferentes páginas web, exploits y ejecutable utilizados por los phishers en este caso concreto ha sido irregular, como suele ocurrir en este tipo de ataques. No obstante las casas antivirus participantes en VirusTotal han obtenido las muestras utilizadas en el phishing que no han detectado y es previsible que en un corto plazo de tiempo ofrezcan protección contra las mismas.

Es por ello que los usuarios, además de contar con la necesaria solución antivirus, deben prestar especial atención en mantener su sistema actualizado, y de forma más especial si cabe el navegador. Además, y dada la corriente de incluir exploits y troyanos en las páginas de phishing, se recomienda a los usuarios que eliminen de forma inmediata cualquier mensaje que sospechen sea un phishing, evitando visitar las páginas preparadas por los phishers.

En cuanto a las entidades, que están trabajando diligentemente en la formación y protección de sus clientes, es recomendable que amplíen su visión de la problemática del phishing y actualicen sus conocimientos sobre las técnicas empleadas por los phishers, ya que existen áreas de oportunidad en la prevención proactiva y mitigación tanto del phishing tradicional como de la generación de troyanos especializados en capturar credenciales.

Bernardo Quintero

21/09/2005 La publicidad web como vía para infectar los sistemas

La publicidad dinámica que muestran las páginas webs a modo de banners o ventanas está siendo utilizada para hacer llegar a los usuarios contenidos maliciosos.

En los últimos tiempos se ha visto una clara proliferación en la utilización de la web como canal para infectar los sistemas y llevar a cabo estafas de todo tipo. Son muchas las páginas que aprovechan vulnerabilidades de los navegadores no actualizados, especialmente Internet Explorer por ser el de mayor implantación, o intentan engañar a los usuarios con distintas tretas para que instalen los programas maliciosos.

Hasta la fecha este tipo de infecciones siempre se achacaba a que el usuario visitaba webs de dudosa procedencia, no confiables. Así los “dialers”, programas que realizan llamadas de tarificación adicional, se solían relacionar con la navegación por páginas webs de contenidos adultos, o los troyanos con la descarga de cracks para juegos y aplicaciones piratas.

Sin embargo a día de hoy se ha diversificado en gran manera los sitios web que pueden contener malware, una simple descarga de un salvapantallas o incluso una aplicación antispyware puede esconder en su

interior un programa malicioso.

A diferencia de los métodos de propagación de malware a través del correo electrónico, donde el programa malicioso llega directamente al buzón del usuario, la infección a través de los sitios webs requiere que el usuario vaya a visitar una página determinada.

Las estrategias para llamar la atención del usuario son variadas, la más habitual consiste en realizar un spam con un mensaje llamativo para que los usuarios al leerlo se sientan atraídos a visitar la página web maliciosa. Con la catástrofe del Katrina se han podido ver varios ejemplos.

Otro de los métodos en boga consiste en hacer llegar los sitios webs maliciosos a los usuarios a través de publicidad. El resultado es que los usuarios, visitando webs confiables, pueden visualizar banners o ventanas que le invitan a instalar supuestas utilidades gratuitas que en realidad esconden malware.

Normalmente los sitios webs donde aparece esta publicidad maliciosa no son conscientes de esta práctica, ya que los banners de publicidad suelen ser gestionados por terceras empresas y se incrustan en sus páginas de forma dinámica.

Esta práctica constituye un riesgo potencial, ya que el sitio web no tiene control sobre los contenidos publicitados. Aunque en los contratos se establece una política de contenidos, lo cierto es que en muchas ocasiones a las empresas de publicidad se les cuelan páginas webs maliciosas, debido a que no existe un control exhaustivo para evitar este tipo de incidentes.

Para ver un claro ejemplo de de como los atacantes están aprovechando la publicidad para intentar instalar programas maliciosos recomendamos ver el caso que describimos del conocido sitio de tiras cómicas dilbert.com en http://blog.hispasec.com/laboratorio/43

Bernardo Quintero

07/10/2005 Planes de recuperación ante desastres

Los recientes incidentes provocados por los desastres naturales, especialmente el huracán Katrina, han puesto de manifiesto lo importante que resulta disponer de un buen plan de continuidad en las empresas cuyos procesos críticos reposan en sistemas de la información.

Es frecuente que muchas organizaciones, desde pequeñas cuentas a las más grandes corporaciones, no contemplen éste tipo de planes, o los eludan en su puesta al día por el simple hecho de que en las zonas de operación no sean frecuentes o sean poco probables eventos indeseables que pudieran tumbar nuestro despliegue informático, como podrían ser los desastres naturales o los ataques terroristas. Muchas veces, una copiosa lluvia puede dejarnos sin actividad, y en lo referente al factor humano, un boicot interno o la acción vandálica de un ladrón podrían ser suficientes para paralizar la actividad de nuestra empresa.

También se considera error pensar sólo en grandes desastres como fuentes de la ruptura de la continuidad: huracanes, tsunamis, terremotos, inundaciones ... son sin duda aspectos a considerar, pero no menos importantes son otros problemas no naturales que podrían dejar en el dique seco nuestras operaciones. Incrementos de la tensión eléctrica, derrames químicos y/o tóxicos en entornos industriales, o la simple acción humana pueden poner en jaque nuestra capacidad de operar, tal y como explicábamos en el párrafo

anterior.

En sistemas de la información, la estrategia más habitual de recuperación es aquella que implica el levantamiento de una réplica de la infraestructura en otro sitio, alejado del emplazamiento habitual, donde haya podido acontecer el desastre. Así hablamos de sitios calientes, templados, fríos y sitios espejo calientes. Hay otra estrategia importante, que es la relativa a la pérdida del personal, pero esa está vinculada a la gestión de recursos humanos, con lo que no entraremos en ella. Tampoco diferenciaremos entre sitios remotos, próximos o instalaciones de recuperación internas, quedando ésta elección a criterio de los responsables implicados.

Los sitios fríos son los indicados para sistemas con alta tolerancia a la indisponibilidad, cuando la recuperación se puede restablecer en dos o tres días. Los sitios templados están indicados para tolerancias de uno o dos días, y los calientes son aquellos emplazamientos cuya tolerancia ante la indisponibilidad es muy limitada, requiriéndose una recuperación total en el plazo de cuatro a 24 horas. Los sitios calientes tipo espejo son los indicados para tolerancia cero ante los tiempos de recuperación, y por tanto, funcionan de un modo paralelo entrando en acción inmediatamente después de que el centro de datos principal haya colapsado. Son por tanto, sistemas redundantes.

Recuperarse ante un desastre no es fácil. Una vez que hemos salvaguardado los datos, toca decidir en qué orden vuelven a la normalidad los procesos abatidos. Normalmente, los procesos que más rentabilidad ofrecen son los que deberían ser activados primero, si bien el orden de la recuperación varía sustancialmente en función de muchos parámetros.

Otra tarea común es la recuperación de las líneas de contacto y de servicio a los clientes, la cual bviamente es vital. La telefonía o los sistemas de atención online a la clientela deben ser rápidamente levantados, por motivos obvios.

Para elaborar un plan de recuperación no existe una metodología fija. Cada cuenta es independiente de las demás en cuanto a sus requisitos de recuperación y los impactos que la discontinuidad puede tener en sus operaciones. No obstante, es frecuente contemplar, al menos, éstos ocho pasos o fases de alto nivel a la hora de establecer una estrategia de recuperación ante desastres:

1) Inicialización del plan. Es el punto de comienzo, donde deberían definirse la meta del plan y los objetivos específicos que sean necesarios.

2) Gestión del riesgo y evaluación de los potenciales emergencias. La única manera de poder ordenar adecuadamente los procesos de recuperación es ordenando previamente los desastres que podemos sufrir, así como la evaluación de los mismos en términos de discontinuidad, así como su impacto técnico-económico en la organización.

3) Preparación para las posibles emergencias, identificado claramente los métodos de recuperación de copias de seguridad y otras técnicas de recuperación colaterales que pudieran ser necesarias.

4) Recuperación tras los desastres, donde deben quedar claramente definidos los pasos a seguir por los equipos de recuperación, especialmente en los casos donde haya riesgo de pérdida de vidas humanas.

5) Recuperación del negocio, ya que una vez aplicado el plan se pretende que el negocio como conjunto vuelva a la normalidad.
6) Pruebas del proceso de recuperación, en las que se pueden diagnosticar fallos y corregir deficiencias en

las fases anteriores.

7) Entrenamiento del personal para el proceso de recuperación, ya que a fin de cuentas, el personal es el que ejecuta los planes.

8) Actualización constante del plan de recuperación, para mantener al día los procedimientos establecidos, así como la lista de emergencias potenciales y su valoración probabilística de riesgo.

Los planes de recuperación son un enfoque que corrige un error frecuente, que es aquel en el que caen muchas organizaciones que estiman que la recuperación consiste únicamente en levantar los backups y paliar los daños en infraestructura. Son sin duda factores importantes, pero no son los únicos.

Y para vencer las reticencias que provoca la inversión en consultoría y mantenimiento de un plan de recuperación, sólo hay que pensar que sucedería si usted perdiera todos sus activos de información y no tuviera posibilidad de recuperarlos, o si no los recuperase a tiempo, o si al recuperarlos los datos no fueran consistentes. ¿Merece la pena?

Sergio Hernando

Entrevista



Mikel Urizarbarrena

Mikel Urizarbarrena ha montado un imperio en una década. Desde Lantek en 1986, pasando por Eurosoft en 1987 hasta Panda Software a principios de los 90, ahora es un referente en cuestión de antivirus, y el único 100% español. Mikel no es sólo el fundador de Panda sino un emprendedor nato que ha sabido enfrentarse a todo con ganas e ilusión.

Hispasec: ¿Cuál y cómo fue tu primer contacto con Hispasec? ¿Estás suscrito a una-al-día? ¿Desde cuándo?

Mikel Urizarbarrena: Creo que mi primer contacto con Hispasec fue a raíz de una comparativa de anti-virus. Por cierto, considero aquella comparativa como la más seria que jamás se ha realizado a nivel mundial. Es muy difícil que alguien dedique tanto esfuerzo y tiempo a hacer una comparativa tan exhaustiva.

Estoy suscrito a una-al-día desde junio de 1999. Es una forma magnífica de estar realmente al día en materia de seguridad informática. ¡Os felicito por estos 10 años de magnífico trabajo!

H: ¿Siempre quisiste tener tu propio negocio? ¿Llegaste a trabajar para terceros o en otras empresas antes de crear Panda?

MU: Sólo trabajé para terceros mientras estudiaba. Una vez que finalicé mis estudios de ingeniería, me incorporé a una incubadora de empresas (Saiolan) y pronto creé Lantek Informática Técnica, empresa dedicada al desarrollo de Software de Diseño y Fabricación asistida por ordenador (CAD/CAM). En 1987 fundé EUROSOFT con la vocación de modernizar la enseñanza y la gestión de las autoescuelas mediante herramientas informáticas...

H: El emprendedor, ¿nace o se hace?. Tres claves/consejos que darías a un futuro emprendedor.

MU: Es posible que algunos nazcan, pero creo que la mayoría de los emprendedores nos hacemos día a día.

Estoy convencido de que todos somos emprendedores en potencia. Por eso mi mensaje a los potenciales emprendedores es que "el hambre agudiza el ingenio y que se pueden crear empresas con poco dinero. Que lo verdaderamente importante es querer hacerlo, descubrir necesidades y formas eficaces de satisfacerlas y abordar el proyecto sin miedo a fracasar".

Para mí emprender es, por encima de todo, una actitud que hace que todo sea más divertido e incluso apasionante. Personalmente creo que los buenos emprendedores son gente sencilla, humilde, apasionados por lo que hacen, muy trabajadores, y con una enorme curiosidad; están interesados en las cosas, más que ellos mismos tratando de ser interesantes.

Mis tres claves serían las siguientes: (1) lánzate a hacer realidad tu sueño sin pensártelo demasiado, (2) corrige el rumbo tan pronto como detectes las necesidades exactas que buscan tus clientes, y (3) persevera y no te amedrentes con las dificultades. Creo que el resto de ingredientes, incluyendo la "suerte", aparecen en escena cuando has hecho lo anterior.

H: ¿Cuantas horas de media trabajas al día? ¿Haces ejercicio? ¿Hobbies?

MU: Trabajo unas 10 ó 12 horas diarias, pero aunque pueda sonar a bastante, me divierto con lo que hago, porque hago lo que quiero, así que más que trabajo, en realidad se trata de juego y diversión. Sí, hago ejercicio. Me encanta el deporte y aunque ya no corro maratones y ultra-maratones como hace unos años, sí que me pego algunas palizas corriendo. También juego al paddle, practico tiro con arco y hago trecking. También tengo otras grandes pasiones: la naturaleza, viajar, todo lo étnico...

H: ¿Cuándo y cómo nace la idea de desarrollar un antivirus?

MU: Fue por casualidad. En 1989 uno de los programadores de EUROSOFT (la empresa dedicada a software para auto-escuelas) me mostró un virus y la verdad es que la "criatura" me fascinó. Inmediatamente nos pusimos manos a la obra para crear ARTEMIS anti-virus. Aquella 1ª versión que presentamos en el otoño de 1990 era eficaz, al tiempo que divertida: incluía una animación cuando "mataba" al "bicho"...

H: ¿Recuerdas cuántos virus aproximadamente detectaba vuestra primera versión de antivirus y cuántas personas formabais Panda? ¿Y actualmente?

MU: Sí, recuerdo perfectamente que Artemis 1.0 era capaz de reconocer 42 virus. Eramos sólo 4 personas, incluyendo a mi mujer, Berta, que se ocupaba de los temas administrativos y financieros. Hoy detectamos más de tres millones de ejemplares y el grupo Panda está compuesto por más de 1.000 personas en 56 países de todo el mundo.

H: ¿Alguna anécdota vírica de aquellos primeros años?

MU: Muchísimas. Aparte de los anti-telefónica y demás virus-protesta, recuerdo una curiosa. En los inicios modificábamos algunos virus, eliminándoles las acciones destructivas, para poder probar la capacidad de detección "en vivo" de los productos, sin correr riesgos de transmisión accidental. Uno de estos virus era

el “Cascade”, también llamado “Falling letters”. “Cascade” era popular porque provocaba que todas las letras que había en la pantalla cayeran progresivamente hacia la parte inferior de la misma, donde se acumulaban.

Pues bien, recuerdo que los técnicos pusieron este “Cascade” inofensivo en el PC de una secretaria, justo cuando teníamos una visita importante. Éramos pocos y estábamos en una sala grande. La secretaria alucinaba cuando las letras empezaron a caer... Ella pensó que estaba infectada y no le pareció muy conveniente mostrar que “estábamos infectados” y se calló. Pasó un mal rato.

H: En estos últimos 10 años, 1998-2008, ¿cómo has visto la evolución de la industria de los antivirus? ¿Cuáles han sido los principales cambios y retos?

MU: Como bien sabes, en el frente del malware hemos pasado de autores que buscaban “fama” a verdaderos criminales con motivaciones claramente económicas. Así, hemos pasado de los virus locales de comienzos de los 90, a las epidemias masivas de finales de los 90 y comienzos del 2000, y a la larga cola de millones de bichos creados con fines económicos: robo de secretos industriales y otros datos confidenciales; robo de credenciales de cuentas bancarias; secuestro de información; etc. Esto constituye un auténtico ataque de denegación de servicios contra los laboratorios de las empresas de seguridad, ya que debemos analizar varios miles de “bichos” al día, cuando no hace mucho eran sólo unas pocas decenas. El malware de hoy es insidioso, imperceptible; a veces global, y otras muy local, afectando sólo a los clientes de una región, o a los clientes de un determinado servicio; a veces efímero, otras diseñado para permanecer años sin ser detectado... El verdadero reto ha sido y es, hoy más que nunca, proteger contra lo desconocido, y eso requiere un acercamiento estratégico y tecnológico muy innovador. En Panda hemos apostado siempre por ello, y así hemos creado tecnologías pro-activas eficaces, como Tru-prevent®.

H: A día de hoy los anti-virus han pasado a ser un “anti-todo”, verdaderas suites de seguridad que van más allá de la detección de todo tipo de malware, con la integración de firewall, antispam, antiphishing, antidialers, etc., lo que también ha traído un mayor consumo de recursos en los sistemas y en ocasiones una mayor interacción con el usuario, quien debe tomar decisiones a petición de la suite. ¿No se está “engordando” demasiado la solución? ¿Debe ser el trabajo de la suite transparente o el usuario debe tener nociones de seguridad para decidir sobre determinadas acciones?

MU: Creo que es responsabilidad 100% de los proveedores de seguridad el evitar y solucionar los problemas de seguridad, sin crear problemas adicionales a los usuarios, y no siempre ha sido así. Muy claramente, es labor de las empresas el desarrollar las tecnologías adecuadas para conseguirlo.

Por supuesto, también es muy recomendable que los usuarios tengan unas nociones mínimas de seguridad informática, de la misma manera que todos tenemos ciertas nociones acerca de cómo mantener una cierta seguridad y evitar robos y demás desastres.

H: Observamos que el Panda ThreatWatch, el indicador de riesgo de infección que aparece en vuestra Web, lleva muchos meses (o incluso más de un año), en nivel naranja-intermedio. Esa situación se repite prácticamente en todos los indicadores del resto de empresas de seguridad. Tras la decadencia de los gusanos de propagación masiva que causaban pandemias puntuales y la aparición de la larga cola del malware (miles de variantes nuevas cada día), ¿sigue teniendo sentido los indicadores de riesgo global? ¿Cómo debemos informar y concienciar al usuario de los peligros reales de infección?

MU: Tienes razón, estos indicadores no son muy útiles hoy en día. Se da la paradoja de que siendo la situación mucho más peligrosa que nunca antes en la historia, el usuario no lo percibe como tal... Vemos como incluso Inteco también comunica sistemáticamente esta dramática situación sin que el mensaje cale demasiado.

Ahora mismo no es fácil informar de forma creíble, porque la situación es de hecho, increíble. Posiblemente lo hayamos hecho mal en el pasado con la profusión de alertas y creo que es humano acabar harto de tanto alarmismo. Al fin y al cabo, las herramientas son sobre todo, para usarse.

Creo que sería más práctico formar a los usuarios en las nuevas amenazas mediante elementos multimedia, que informar una y otra vez de todo lo nuevo que acontece. Un usuario formado, será seguramente también un usuario informado.

H: Siguiendo con las herencias del pasado, la mayoría de certificaciones y algunas comparativas se basan en la lista in-the-wild (los virus más extendidos). ¿Tiene sentido mantener esa lista y seguir utilizándola como patrón de las evaluaciones antivirus? A grandes rasgos, ¿cómo deberían evolucionar las certificaciones y comparativas?

MU: Tal y cómo funciona la lista in-the-wild hoy en día tiene una utilidad escasa. En el pasado ha sido un instrumento muy útil tanto para usuarios como para desarrolladores, pero se ha quedado obsoleta y ha sido ampliamente superada por la situación del malware. Como decía antes, hoy en día el malware es imperceptible e insidioso, y muchas veces también efímero, dejando de funcionar en pocas horas. Al mismo tiempo hemos asistido a una gran proliferación de troyanos e incluso rootkits, y estos no aparecen reflejados en la lista in-the-wild. A mi modo de ver esto requiere que la lista in-the-wild: (1) pase de ser una lista de virus, a una lista de malware, y (2) que se actualice prácticamente en tiempo real. Desde 2006, en Panda venimos luchando por conseguirlo, promoviendo la colaboración entre los diversos agentes públicos y privados. No es un tema sencillo, pero puede y debe hacerse.

Tanto las certificaciones, como las comparativas, deberían estar diseñadas para proporcionar a los usuarios una garantía de si el producto en cuestión puede protegerle adecuadamente o no frente al malware en circulación en ese momento. Esto debería ser monitorizado continuamente, de forma que se vea la evolución de la protección que ofrece cada producto y fabricante. Esto requiere un esfuerzo enorme, pero no sería posible hacerlo sin tener un muestreo en tiempo real de qué malware está afectando realmente a los usuarios de cada región. Creo que tenemos que comenzar por ahí.

H: En los últimos tiempos han existido cambios importantes en Panda, especialmente con la entrada de fondos de inversión al accionariado. ¿Cuál es tu puesto y función actualmente en Panda?

MU: Tras la entrada de los fondos de inversión en la compañía mi posición pasó a ser la de Presidente del Consejo de Administración. Colaboro en la planeación de la estrategia del grupo.

H: Al margen de tu trabajo en la industria de la seguridad, ¿a qué dedicas más tiempo últimamente?

MU: Hace tres años inicié una start-up en el campo de la semántica. Estamos a punto de lanzar las primeras soluciones. También estoy arrancando una Empresa social que tiene que ver con crear puestos de trabajo en países en vías de desarrollo. A nivel más personal acabo de tener un hijo y esperamos incrementar la familia con un par de niños adoptados.

H: ¿Cuál es el sitio más interesante en el que has estado por trabajo? ¿y por hobby?

MU: Por trabajo, en el Silicon valley. Es un hervidero de pasión y actividad creativa. Por hobby, la selva centro-africana donde viven los pigmeos baká. Tal vez para no olvidar las raíces... Me apasiona ese contraste entre lo más avanzado y lo más primitivo.

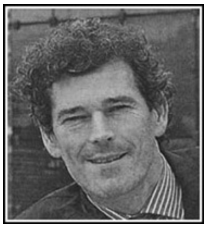
H: El último libro que has leído

MU: "Un mundo sin pobreza" de Muhammad Yunus. Me ha llamado poderosamente la atención su concepto de "Empresa Social": una empresa mercantil que debe generar beneficio que se reinvierte totalmente en su finalidad, exclusivamente social.

H: ¿Cómo te ves dentro de diez años?

MU: Hace ya muchos años tomé la firme decisión de que cuando fuera más mayor diría que hice esto y que me salio bien; también que hice esto otro y no me salió tan bien; pero me juré a mi mismo que no diría, ni pensaría "si hubiera hecho" o "pude hacer, pero...". Nada de lamentos, ni "sies" condicionales...

Espero sentirme muy satisfecho de haber hecho todo lo que estuviera a mi alcance en esos 10 años. También espero tener proyectos ambiciosos y que me llenen para los 10 años siguientes...



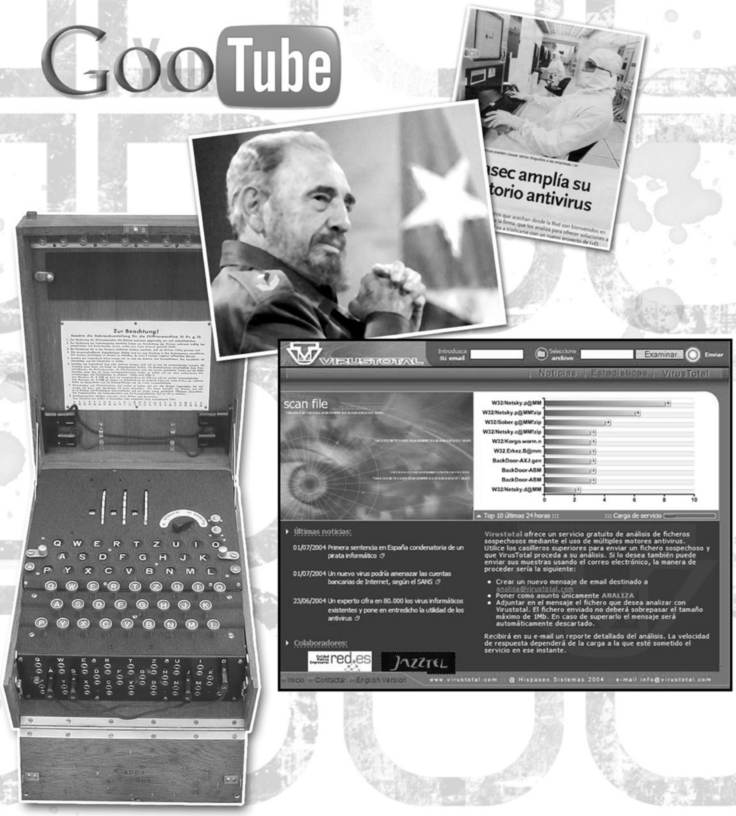
Capítulo 8

AÑO 2006

7D6

3726

1111101010110



1152748800 – 1215907199

Durante este año...



_ El 1 de enero entra en vigor en España **la nueva ley antitabaco**, que impide fumar en la mayoría de sitios públicos que no posean una infraestructura adecuada ni en los lugares de trabajo.

_ En Sidney, Australia, se llega el 1 de enero a los **45 grados centígrados**, su día más caluroso hasta la fecha.

_ Se establece que el 3 de enero de 2006 internet alcanza los **mil millones de usuarios** en todo el mundo.

_ Aunque es identificada por primera vez en Italia a principios del siglo XX , se comienza a crear histeria en todo el mundo a raíz de ciertos brotes aislados de **gripe aviar** en Europa, Medio Oriente y África. Las noticias provocan un dramático descenso de consumo de productos avícolas. Se establecen restricciones en el comercio y caen los precios. Tiene suficiente potencial como para infectar a distintas especies de mamíferos, como por ejemplo el cerdo y el gato, pero se cree en principio que es imposible o muy improbable la transmisión entre humanos, necesitando contacto directo con las aves para su contagio. Sin embargo en junio se comprobaría un caso real de transmisión del virus entre personas.

_ Finaliza con éxito la misión espacial de la NASA que pretendía recoger **polvo espacial** de un cometa.

> En febrero se desata la polémica sobre las **caricaturas de Mahoma** expuestas en un periódico danés. El mundo islámico protesta enérgicamente contra la reproducción en diarios europeos de dibujos y caricaturas del profeta, por considerarlas ofensivas. Las doce caricaturas de Mahoma que inician el grave conflicto diplomático son publicadas por el diario danés Jyllands-Posten y reproducidas por otros periódicos de Europa en los días siguientes. Los países islámicos prohíben la venta de los diarios donde hayan sido publicadas. En uno de los dibujos aparece Mahoma vistiendo un turbante con forma de bomba clásica con la mecha encendida. En otra viñeta, un cuadro de diálogo asegura que se está quedando sin vírgenes. El diputado independiente holandés Geert Wilders sube a su página web las polémicas caricaturas sobre Mahoma. Califica de "muy preocupante" que los dibujos desataran la ira entre los musulmanes. Las publica para mostrar su apoyo a sus creadores. Como resultado es amenazado de muerte por integristas.

_ El 3 de febrero la Frikipedia es retirada temporalmente de Internet tras una denuncia de la SGAE. La **"Frikipedia"** nace como una parodia de la Wikipedia. Entre sus definiciones, se incluye una irónica descripción de la Sociedad General de Autores y Ejecutantes (SGAE). Pero según Pedro Farré, director de Relaciones Institucionales de la SGAE, constituye una "clamorosa difamación". Al recibir la demanda, el autor de la web la cierra y pide ayuda económica a la comunidad internauta, para sufragarse un abogado. Más de 200 webs secundan una sonora campaña de apoyo. Entre los internautas y la SGAE se tensa aún más si cabe la relación. Aparecen pintadas ofensivas en la fachada de la sede de la entidad. Un programador descubre que el sistema

de envío de comentarios de la web de la SGAE tiene un filtro que bloquea palabras “malsonantes”: “Linux” entre ellas. Es un pequeño escándalo en la comunidad de Internet. Farré lo califica de “anécdota ridícula” y continúa: “Hace cinco años, cuando hicimos este filtro, Linux se asociaba a movimientos alternativos y a insultos. Olvidamos retirarla, pero se retirará”. La demanda contra la Frikipedia también sería retirada.

_ La Wikipedia en inglés edita su **artículo número 1.000.000.**

_ En marzo se encuentra muerto a **Slobodan Milosevic** en su celda de la prisión del Tribunal Penal Internacional. Era juzgado en La Haya por crímenes de guerra y genocidio por su responsabilidad en los tres conflictos de los Balcanes (Croacia, Bosnia y Kosovo) durante toda la década de los 90 y que causaron más de 200.000 muertos. El juicio comenzó en febrero de 2002 y había sido interrumpido en numerosas ocasiones por los problemas de salud del acusado. Pasaría a la historia como el primer ex Jefe de Estado que comparecía ante un tribunal internacional.

_ ETA anuncia un **alto el fuego permanente** a partir del día 24 de marzo de 2006. Son momentos de esperanza para la paz. Sin romper oficialmente el alto el fuego, el 30 de diciembre de ese mismo año haría estallar un artefacto en el aparcamiento de la Terminal 4 del Aeropuerto de Barajas de Madrid. En junio de 2007 se rompería la tregua oficialmente en un comunicado publicado en la página web del diario Berria. Los terroristas argumentarían que “no se dan las condiciones mínimas para seguir con un proceso de negociación” y que el Gobierno de Zapatero “ha respondido al parón de las acciones armadas, con detenciones, torturas y persecuciones”.



_ Durante el verano, **Fidel Castro delega** el poder en su hermano Raúl. Castro se encuentra en un delicado estado de salud. Incluso se rumorea que podría estar muerto. Aparecería varias semanas después con su famoso chándal. Se enviarían posteriormente por email varias oleadas que contienen bulos sobre vídeos y noticias de su muerte, que esconderían en realidad malware.

_ Después de algunas detenciones en Londres, relacionadas con terroristas que pretendían viajar desde esta ciudad hacia los Estados Unidos, los **líquidos y geles se prohíben** en el equipaje de mano de los vuelos comerciales.

_ En agosto, y más de 70 años después de ser descubierto, **Plutón** es degradado de “planeta” a “planeta enano” por la asociación internacional de astronomía en su vigésimosexta asamblea general.

_ El 23 de agosto encuentran sana y salva a **Natascha Kampusch**, desaparecida en marzo de 1998 en extrañas circunstancias y con solo 10 años de edad. Durante su secuestro vivió en un zulo a 2,5 metros de profundidad y sólo 5 metros cuadrados, sin luz natural en el sótano de la casa de su raptor Wolfgang Priklopil. Tenía “permisos” ocasionales para salir al jardín. Al parecer Priklopil la educó durante ese tiempo. Amenazaba a Kampusch con matar a quien pidiera ayuda o suicidarse si escapaba. Natascha huye durante una de sus salidas del zulo y, antes de que lo encuentren, Priklopil se suicida saltando a las vías de un tren. Natascha se convierte en un fenómeno mediático. Se abre una cuenta para financiar el tratamiento de sus traumas y comienza a ofrecer entrevistas millonarias, que se supone dona a instituciones caritativas.

_ El 3 de septiembre la selección española de baloncesto, sin poder contar con Pau Gasol lesionado en la semifinal, gana el campeonato del mundo contra Grecia, en un cómodo partido que termina 70 a 47. En la semifinal había vencido a Argentina gracias a un apretado 74 a 75.

El 10 de octubre **Google compra YouTube** por 1.650 millones de dólares. Google Video es un fracaso, no consigue ni la popularidad ni las funcionalidades técnicas que han hecho de YouTube un fenómeno social. YouTube había nacido apenas año y medio antes, en febrero de 2005 y en cuestión de meses se convierte en una marca mundialmente reconocida en la web, que no deja de innovar e incluir nuevas funcionalidades. Chad Hurley y Steve Chen emiten a través de su página un vídeo en el que, de forma informal, se muestran exultantemente alegres ante la compra.

_ El 28 de octubre **Televisión Española celebra los 50** años del comienzo de sus emisiones en España, y una-al-día, su octavo cumpleaños.

_ Estados Unidos llega a los **300 millones de habitantes**.

_ En octubre Microsoft publica Windows **Internet Explorer 7**. Han pasado 5 años exactos desde la aparición de la versión anterior. La guerra de navegadores ha comenzado hace tiempo y Microsoft decide trabajar en un producto que tenía desastrosamente abandonado. Ofrece por fin características programadas en otros navegadores desde hace años, como la navegación por pestañas o lector RSS integrado. Llega en un momento en el que prácticamente todos los navegadores se ven afectados de una manera u otra por distintas vulnerabilidades.

_ El 3 de noviembre la revista Science predice que el 90% de las formas de vida marítimas estarán **extinguidas** en el 2048.

_ El 30 de noviembre sale **Windows Vista** para ser comprado por licencias de distribuidores.

_ El 30 de diciembre **Saddam Hussein** es ahorcado en Baghdad. Las imágenes de su ejecución son recogidas por un teléfono móvil y distribuidas por las redes P2P.

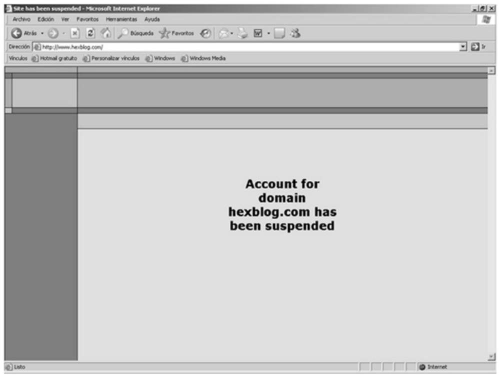
_ Ese mismo día tiene lugar el **atentado en el aeropuerto de Madrid-Barajas**. ETA hace estallar una bomba en el aparcamiento “C” en la Terminal 4 de Barajas. El resultado es de 19 heridos leves y dos ciudadanos de nacionalidad ecuatoriana fallecidos..

Seguridad Informática



Microsoft publica un aviso de seguridad donde confirma la existencia de la vulnerabilidad WMF **(Windows Meta File)** en Windows. El fallo permite la ejecución de código de forma transparente y con sólo visitar una página web. Está siendo aprovechado activamente para infectar los sistemas de forma masiva. Prácticamente todas las versiones de Windows se ven afectadas. Aparecen todo tipo de exploits más potentes, capaces de presentarse bajo otros formatos de imágenes (jpg, gif...) y generar código polimórfico que dificulta su detección genérica por parte de los antivirus, IDS, y resto de soluciones basadas en firmas. Se popularizan los correos que incorporan una imagen especialmente manipulada que aprovecha el fallo, pretendiendo felicitar el nuevo año. La fecha oficial en la que Microsoft pensaba publicar sus parches es el 10 de enero, más de una semana después de la detección. En ese tiempo la situación podría

volverse insostenible. Ilfak Guilfanov, autor del popular desensamblador IDA, publica un parche no oficial que soluciona el fallo. Su web hexblog.com se ve completamente saturada ante la avalancha de descargas y permanece inactiva durante varias horas. Steve Gibson insinúa que el problema es tan absurdo y lleva ahí desde hace tanto tiempo, que podria ser intencionado.



Ante las presiones, Microsoft publica un parche fuera de su ciclo habitual de actualizaciones los segundos martes de cada mes, y el día 5 aparece la solución oficial. Esta actualización soluciona el problema de la ejecución de código, pero no el de denegación de servicio. Distintas versiones del parche solucionarían por completo este gravísimo incidente.

_ El 19 de enero se cumplen 20 años de la aparición del **virus Brain**, primer ejemplar para la plataforma PC. Antes de ese Brain, en noviembre de 1983, Fred Cohen acuñó el término "virus" y demostró empíricamente lo que todos temían e intuían: efectivamente, como muchos habían estudiado teóricamente, se podía crear código que atacara a otros programas modificándolos, y a la vez fuese capaz de auto-replicarse. Cohen presentó el código del experimento en su doctorado para la Universidad del Sur de California y demostró al mundo que este comportamiento era posible en un programa implementándolo en una máquina Vax (bajo Unix). El programa creado podía hacerse con los derechos de los archivos del sistema en menos de una hora, con un tiempo récord de cinco minutos. El hecho causó tanto miedo que se prohibieron este tipo de prácticas, pero la curiosidad y fascinación crecía en los nuevos informáticos, que comenzaron a experimentar con nuevos "programas" y los recién estrenados sistemas. Nacían los primeros virus.



_ Se detecta un troyano que se distribuye por correo basura, **simulando provenir de VirusTotal**. Está dirigido a usuarios brasileños. La excusa esta vez es avisarles de que están infectados con un virus, W32.Jeefo@mm, y ofrecer un enlace para que se descargue una vacuna genérica para desinfectarse (que en realidad es el troyano). Una vez más se aprovecha la imagen de una reputada web para dar confianza a las víctimas.

_ En febrero se detecta la distribución por todo el mundo de un nuevo gusano, que debido a los textos que incluye recibe el imaginativo nombre de **"Kama Sutra"**. A pesar de ser "otro más" de los gusanos que aprovechan la ingeniería social para infectar a sus víctimas, consigue una cobertura importante en medios especializados. El autor del virus consigue con creces lo que probablemente pretende: la atención incondicional de los medios, miles de noticias escritas sobre él y la inquietud de muchos usuarios horas antes del día 3 de febrero, supuesto momento de activación de su código maligno. Una vez infecta el sistema, intenta desactivar el funcionamiento de diversos productos antivirus, recoge direcciones de correo en el ordenador de la víctima para distribuirse por e-mail utilizando su propio motor SMTP, y también intenta distribuirse a través de los recursos compartidos. Lo que provoca que se le tome en cuenta es que los días 3 de cada mes el gusano sobreescribe (que no borra) archivos con extensiones .doc, .xls, .mdb, .mde, .ppt, archivos comprimidos con .zip y .rar, .pdf, .psd y .dmp. Destruye documentos muy valorados por todo tipo de usuarios y que suelen contener información importante para su trabajo, estudios o cualquier otra actividad. Hoy en día, pocos son los virus que se dedican a destruir

de alguna forma el sistema en el que se han alojado. Otro detalle que lo lleva a ser tan popular es el exótico nombre adoptado por algunas casas antivirus para diferenciarlo. No ha existido un consenso claro, y, entre otros, al virus se le ha llamado Nyxem, BlackMal, Kapser, MyWife, Tearec... pero "Kama Sutra" ha resultado ganador en los medios no especializados, y eso que "Kama Sutra" era simplemente uno de las decenas de asuntos que aparecían en los correos infectados. El sexo siempre será un reclamo fácil para intentar que usuarios despistados ejecuten archivos que vienen de fuentes no confiables, y esta vez no es una excepción.

_ El 14 de febrero algunos empleados de la compañía "The Trainning Camp" entregan en mano, a viandantes que acudían a su lugar habitual de trabajo, un CD bajo la excusa de que el disco contenía información sobre una promoción especial motivada por el día de San Valentín. Los compactos contienen en realidad un simple código que permitía informar a la compañía de quién había ejecutado el programa en su interior. Entre ellos se encontraba personal de grandes bancos y aseguradoras multinacionales. Lo más grave es que en la carátula del CD **se advertía claramente sobre los peligros de la instalación de software** de terceros no confiables, y de que el hecho de hacerlo podría suponer una violación de las políticas de seguridad del lugar donde se instalase.



_ Durante febrero y marzo, escalonadamente, **Hispasec se muda** a unas oficinas más grandes, cerca de su sede anterior. Las vistas son envidiables.

Un equipo de investigación, apoyándose en computación distribuida, consigue descifrar un mensaje de un total de tres que llevan más de 60 años en la oscuridad al estar cifrados con una variante de la **máquina Enigma**. Fueron interceptados en el Atlántico Norte en 1942. 64 años después comienzan los resultados tangibles en las labores de descifrado. Este legendario aparato se caracterizó por poder cifrar y descifrar mensajes de forma robusta, siendo totalmente transportable. Dotada de una serie de rotores mecánicos, Enigma comenzó a comercializarse en la década de los años 20, aunque fue el uso intensivo que le dieron desde la Alemania Nazi el factor que la covirtió en un instrumento muy conocido, por las evidentes implicaciones históricas del uso bélico de la máquina. La versión militar, llamada Wehrmacht Enigma, fue protagonista, durante la Segunda Guerra Mundial, de una encarnizada lucha por parte de criptoanalistas aliados para descifrar los mensajes capturados. La revelación de ULTRA (nombre código asignado a los resultados del descifrado de las comunicaciones alemanas) es considerada hoy en día un factor crítico para acelerar el fin de la guerra en un período estimado de uno a dos años. Muchas comunicaciones de la inteligencia alemana fueron capturadas y descifradas por los aliados, lo que según los historiadores, otorgó significativas ventajas en la estrategia militar del conflicto. Muy poco después se descifraría el resto de mensajes.



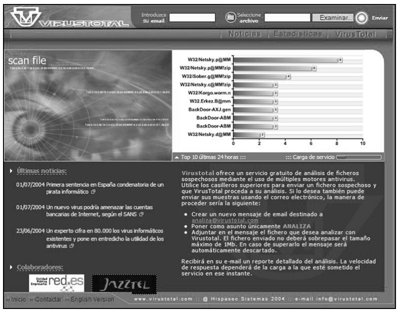
_ Se sufre una pequeña epidemia de **Commwarrior** en España. Muchos usuarios reciben a través de bluetooth malware que afecta a los más avanzados móviles de marca Nokia.

_ En marzo **"Guillermito"** pierde finalmente la apelación en el juicio con Tegam. Es obligado a pagar 15.000 euros. Tras no pocas vicisitudes, el 7 de junio de 2005 la justicia francesa condenó a Guillaume al

pago de 14.300 euros. En realidad la cantidad es mínima en comparación con la petición de la acusación, 900.000 euros, que consideraban era sólo el 10% de los daños reales que habían sufrido. Guillaume ironizaba con el hecho de que supuestamente habría hecho perder 9 millones de euros a una empresa cuyo volumen de negocio en 2003 era de 1.4 millones de euros. Guillaume T. comenta “No se tiene derecho en Francia a demostrar técnicamente que un programa informático presenta vulnerabilidades de seguridad o que su publicidad es falsa. Duerman tranquilos, ciudadanos, todos sus programas informáticos son perfectos”. En Francia está prohibido solicitar dinero para pagar una multa así que Guillaume, que no dispone de tal cantidad, pide a la comunidad donaciones para comprar “un antivirus nuevo”. Mediante una campaña de donaciones a través de PayPal se recauda con creces la cifra necesaria. El remanente sería destinado a caridad.

_ Karpersky anunciaba una prueba de concepto capaz de infectar tanto a sistemas operativos Windows de Microsoft como GNU/Linux en general. Lo llama **Virus.Linux.Bi.a/Virus.Win32.Bi.a**, y vuelve a alertar sobre la posibilidad de que el mercado de los virus se abra para ambas plataformas. Bastante inofensivo, sólo se extiende sobre los archivos en el directorio donde se haya ejecutado, no causa daño alguno y no se autopropaga a otros sistemas. Su peculiaridad es que es capaz de infectar dos tipos de ejecutables distintos, los PE (Portable Executable) que son los ejecutables que usa Windows, y los ELF (Executable and Linkable Format) que es el formato estándar binario para Linux.

_ El 21 de abril nace el **blog específico de VirusTotal**. Se publicarán anuncios de nuevas funcionalidades, motores, y noticias del sector en general.



Es un año de importantes **cambios para VirusTotal**. A mediados de 2006 ya procesa el millón de muestras mensuales recibidas de forma sostenida. Esto requiere un aumento y modificación de infraestructura interna, además de una ampliación importante de los recursos utilizados por el servicio en sí. También se facilita el uso por web. El funcionamiento original consistía en dejar a la espera al usuario para presentar los resultados completos una vez se había terminado de hacer el análisis. El nuevo interfaz de respuestas es mucho más informativo en la fase previa, dando desde la posición en la cola de espera hasta tiempos estimados para el comienzo del análisis. Una vez en fase, los resultados presentados por los motores se dan en tiempo real. El nuevo interfaz web ofrece información extra al usuario, incluye hashes del archivo analizado, empaquetadores detectados por algunos de los motores, y el resultado de la Sandbox de Norman en caso de detecciones heurísticas. Estos datos son muy apreciados por usuarios avanzados del servicio que buscan un mayor detalle sobre la muestra analizada. La demanda se multiplica por cinco desde principios de 2005. En esos momentos el número de muestras analizadas en el servicio rondaba las 20.000 diarias, a finales de 2008 se está sosteniendo la cifra de 60.000 análisis al día.

_ En mayo Steve Wiseman descubre, casi por casualidad, una importante **vulnerabilidad en VNC**. Se trata de un software de administración remota muy usado en distintos sistemas operativos que permite interactuar con el escritorio de cualquier sistema. El fallo puede hacer que se eluda de forma sencilla la autenticación y acceder al equipo con el servidor instalado sin necesidad de conocer la contraseña. Aparecen numerosas herramientas que permiten escanear la red en búsqueda de versiones vulnerables.

Entrar en sistemas remotos se convierte, durante algunas semanas, en un juego de niños.

_ Aunque Yahoo, AOL y Microsoft junto con el gobierno del Reino Unido anunciaron en 2003 una **estrategia diseñada para combatir el spam** tanto de forma conjunta como por separado, la basura sigue creciendo. Establecerían estándares técnicos para combatir la amenaza e intentarían promover nuevas leyes que perseguirían y castigarían de forma más severa a los infractores. Desde entonces, exceptuando casos más o menos sonados, el envío de correo basura sigue siendo algo poco perseguido. Las leyes dejan de ser eficaces en el momento en el que enviar spam puede ser una actividad descentralizada, llevada a cabo desde cualquier punto del planeta contra cualquier país, delegada en millones de máquinas secuestradas y encubiertas bajo direcciones falsas. La situación era más preocupante hace algún tiempo. En diciembre de 2002 se anunciaba ya que el 40% de los correos que circulaban por Internet eran basura. En junio de 2003 se llegaba a la salomónica situación de un 50% de correo inútil entre todo el tráfico circulante. Ryan Hamlin, jefe del grupo antispam de Microsoft, declaraba por aquellas fechas que las nuevas medidas legales que se estaban diseñando, provocarían un ligero descenso de esta tendencia para finales de 2004 o comienzos de 2005. En 2006 llega a más del 60%. Años más tarde se frenaría la velocidad de subida (más que nada por las cifras que se están alcanzando) pero la tendencia sigue siendo al alza, llegando a picos del 80 y 90% de basura en todo el correo mundial recibido.

_ Durante todo el verano se encuentran numerosas vulnerabilidades **"0 day" en productos de Microsoft Office**. Se detectan ataques que aprovechan vulnerabilidades desconocidas públicamente y para las que no existe parche. Se trata de fallos que permiten atacar cualquier sistema, puesto que la detección por parte de las casas antivirus de este tipo de documentos infectados es escasa. Al contrario que la mayoría del malware, que suele ser genérico y lanzado indiscriminadamente contra cualquiera que posea un sistema desprotegido, se popularizan las amenazas directas a compañías que reciben este intento de infección. Se trata de ataques perpetrados especialmente contra ellos. No se sabe durante cuánto tiempo han podido aprovechar estos fallos. A razón de casi una o dos vulnerabilidades por mes en Word, Excel o PowerPoint, es un verano negro para Office. Además, los ataques con nuevos fallos se detectan muy poco tiempo después del segundo martes de cada mes, con lo que habitualmente es necesario esperar casi todo un mes para que Microsoft cumpla su siguiente ciclo de actualizaciones y poder estar protegido. Se observa un claro cambio de tendencia en la forma en la que aparecen estos problemas, unida a una obsesiva y oportunista fijación contra este software de Microsoft.

_ En mayo se empiezan a conocer las mejoras de seguridad que incluiría Windows Vista, como por ejemplo que implementará **ASLR (Address Space Layout Randomization)** activado de serie. En la beta 2 de Windows Vista se incluye una nueva funcionalidad destinada a prevenir la ejecución de código no deseado en el sistema a través de, habitualmente, desbordamientos de memoria intermedia. Cuando ocurre un desbordamiento de memoria, el espacio de direcciones de memoria del sistema operativo se corrompe de alguna forma. Si un atacante, a través de cualquier vulnerabilidad, es capaz de sobrescribir ciertos valores, puede tomar el control del sistema y hacer que se ejecute cualquier parte de la memoria (con el código que contenga). Es habitual que los atacantes "se ayuden" de ciertas direcciones de memoria conocidas para poder "saltar" en el espacio de memoria y ejecutar su código inyectado. Estas direcciones coinciden habitualmente con las librerías básicas del sistema operativo, que son siempre cargadas en el mismo espacio de memoria. Así los exploits, programados con una dirección concreta, funcionan siempre en las mismas versiones de Windows, pues saben exactamente dónde ir para poder ser ejecutados porque los procesos principales siempre se cargan en el mismo espacio. Esta facilidad para predecir las direcciones comunes es precisamente el punto que ataca ASLR. Cada vez que se arranca el sistema el método se ocupa de cargar las áreas críticas del sistema en espacios más o menos aleatorios, de forma que no pueden ser predichas de forma sencilla. Al menos, un atacante tendría que probar un número significativo de valores

(hasta 256) para poder acertar con la dirección adecuada. Incluso así, este valor no sería el mismo en cualquier otro sistema Windows Vista, por lo que un sistema automatizado de ataque (por ejemplo un gusano) tendría que adivinar en cada sistema atacado la dirección concreta. Durante la **Black Hat de 2008**, se demostraría un método para saltarse esta y otras medidas de seguridad de Vista.

_ En junio se da a conocer que HP ha hospedado en su página web, durante un tiempo indefinido, uno de **sus controladores de impresora infectado por FunLove**, un virus de 2001. BitDefender alerta de la situación y HP se ve obligada a retirar de sus servidores un controlador para la impresora de HP "Officejet g85 All-in-One" en su versión coreana para Windows 95/98 por contener el virus FunLove. Al parecer HP tropieza en la misma piedra, pues ya sufrió la embestida de este virus anteriormente, y fue distribuido también con una versión japonesa de uno de sus controladores. Un año después (en 2002), a Microsoft le pasó exactamente lo mismo... incluso con el mismo virus FunLove.

_ **Joanna Rutkowska** presenta a mediados de 2006 su **Blue Pill** y causa un gran revuelo y confusión. Rutkowska, experta en rootkits, aprovecha una nueva funcionalidad de los procesadores AMD para crear un rootkit indetectable en cualquier sistema operativo. AMD incluye una tecnología llamada SVM/Pacifica destinada a optimizar la virtualización a bajo nivel desde el procesador. Forma parte de los Athlon 64 y Turion 64 bits. Rutkowska crea una prueba de concepto que demuestra que cualquier sistema operativo que use este hardware tiene un serio problema: el software puede asumir un rol llamado "hypervisor". Este



concepto se refiere a un nivel superior incluso al supervisor, que es el nivel al que corre el sistema operativo. Por hacer una comparación, VMware corre a un nivel hypervisor, mayor incluso que el sistema operativo que aloja. Esto, trasladado al hardware, hace que cualquier sistema operativo pueda tener un rootkit indetectable. Las pruebas que realiza Joanna son sobre Windows Vista (en beta en ese momento). Invalida lógicamente la medida de prevención de Vista 64 bits que impide que en el kernel se ejecute software no firmado digitalmente. Los medios creen erróneamente por tanto, que sólo afecta al sistema de Microsoft.

_ HD Moore tiene una ocurrencia imitada hasta la saciedad. **"El mes de los fallos en..."** Durante todo julio, se dedica a publicar una vulnerabilidad al día, referente a los navegadores y desconocidas hasta el momento. La idea tiene tanto éxito que sería copiada durante meses. Se piensa que el fallo que corresponde con el día 17 de julio (como la mayoría) es una denegación de servicio. Hubo que esperar al 27 de septiembre para que alguien hiciese pública una forma de aprovecharlo para ejecutar código y se convirtiese en una de las vulnerabilidades más explotadas del momento.

En julio la compañía **SoftScan** publica un estudio sobre el correo. Los cinco primeros puestos de familias de virus en junio y su porcentaje de presencia en correos infectados es:

1.- Phishing: 48.05%, **2.**- Netsky: 16.69%, **3.**- Mytob: 15.05%, **4.**- Bagle: 5.94%, **5.**- Mydoom: 3.44%

El primer puesto lo ocupan los virus (o malware en general) destinados al phishing. En esta categoría se englobaría todo tipo de código destinado a robar credenciales bancarias, ya sea registrando teclas, robando información, engañando al usuario... pero siempre desde el punto de vista de la rentabilidad y el lucro. Nada menos que casi la mitad del malware que circula en junio corresponde a este tipo de basura.

_ En julio se anuncia que **Microsoft compra SysInternals**. Históricamente se trata de herramientas técnicas para Windows muy populares y usadas por especialistas: monitores de comportamiento de archivos, de registro, un excelente explorador de procesos, y un largo etcétera. Mark Russinovich, creador de SysInternals (que parecía conocer la programación de Windows mejor que los propios desarrolladores oficiales) pasa a la plantilla de Microsoft. SysInternals ofrecía no solo las herramientas sino también su código fuente. Se especula sobre la desaparición de las herramientas y la página sufre una avalancha de visitas buscando un código que se supone desaparecerá. Microsoft seguiría ofreciendo de forma gratuita las herramientas, y su desarrollo continuaría adelante, ya sin ofrecer además el código fuente.

_ En agosto un **banner de publicidad alojado en MySpace** consigue infectar a más de un millón de usuarios de Windows gracias a una vulnerabilidad para la que existía parche desde enero de 2006. MySpace no tiene, en principio, responsabilidad directa sobre el incidente. El malware se ejecuta sin permiso, a través de la vulnerabilidad WMF, parcheada por Microsoft en enero de 2006. Bernardo Quintero, en septiembre de 2005, ya analizó una situación parecida, en la que una publicidad en la página de la tira cómica de Dilbert intentaba infectar con el adware Winfxer 2005.

_ Durante la DefCon de este año Collin Mulliner demuestra que es posible desarrollar **un gusano que infecte los dispositivos móviles basados en Windows CE** de forma automática y transparente, sin la necesidad de que el usuario intervenga. La prueba de concepto es posible gracias a una vulnerabilidad en el procesamiento de mensajes MMS (Multimedia Messaging Service).

_ En VirusTotal se detectan varios **troyanos que realizan un vídeo de la pantalla del usuario** mientras este se autentica para entrar en su cuenta bancaria por Internet. Esta funcionalidad representa un salto cualitativo en la peligrosidad de los troyanos bancarios, y en especial contra los teclados virtuales implantados por muchas entidades. Como suele ocurrir cuando una medida de seguridad como los teclados virtuales se generaliza, no tardan en aparecer troyanos bancarios que burlan este tipo de protección. Desde aquellos que directamente se inyectan en el navegador y capturaban el usuario y contraseña antes de que sean enviados por HTTPS al servidor de la entidad, hasta los que fueron programados específicamente contra los teclados virtuales y se activan al hacer click con el ratón, almacenando la posición del cursor o realizando pequeñas capturas de pantalla. Hispasec publica un popular vídeo demostración que obtiene una gran repercusión.

_ En septiembre, se descubre que **el SMiShing** llega a España. Panda alerta a finales de agosto de un nuevo virus que se distribuye a través de correo electrónico y convierte a los sistemas infectados en equipos zombi. Las víctimas no reenvían correos electrónicos, sino mensajes cortos a móviles españoles.

_ El día 19 de septiembre **Symantec anuncia una nueva vulnerabilidad** desconocida en PowerPoint que permite la ejecución de código arbitrario y que está siendo activamente aprovechada. Ante la avalancha de este tipo de noticias que azotan a Microsoft ese verano, todo apunta a que se trata de un nuevo "0 day", vulnerabilidad sin parche explotada de forma masiva. En esta ocasión las alarmas suenan de forma precipitada, y sobre todo, antes de un buen análisis del problema.

_ Ante tanto "0 day", se popularizan los parches no oficiales para Microsoft. Se descubre una vulnerabilidad basada en la funcionalidad **VML (Vector Markup Language)** del navegador Internet Explorer que permite la ejecución de código con solo visitar una página. Necesita soluciones porque está siendo aprovechada de forma masiva. Un grupo de reputados expertos (entre los que se encuentra Ilfak Guilfanov, programador del exitoso primer parche no oficial para la vulnerabilidad WMF) crea la organización ZERT (Zero Day Emergency Response Team). Su objetivo desde entonces es el de programar parches para solventar problemas de seguridad de tipo "0 day" siempre que su gravedad lo requiera. ZERT

no pretende reemplazar a los parches oficiales. Según ellos, sólo ofrecen una alternativa en un momento de crisis. El día 27 de septiembre, fuera de su ciclo oficial de actualizaciones, Microsoft publicaría el parche oficial para solucionar definitivamente la vulnerabilidad.

_ Hispasec descubre y analiza un nuevo **troyano bancario dirigido a entidades españolas y latinoamericanas**, que combina la captura del teclado físico con una técnica optimizada para los teclados virtuales. Está diseñado específicamente contra los usuarios de diversas entidades de Argentina, Bolivia, Brasil, Cabo Verde, España, Estados Unidos, Paraguay, Portugal, Uruguay y Venezuela.

_ Mischa Spiegelmock y Andrew Wbeelsoi muestran en la conferencia ToorCon una vulnerabilidad en Mozilla Firefox que puede permitir a un atacante remoto ejecutar código arbitrario en el contexto del usuario que ejecutase la aplicación, independientemente del sistema operativo sobre el que se asiente. No se publican más detalles técnicos sobre el problema, pero la revelación de los descubridores llama la atención de los medios. Poco después los propios responsables de la difusión del supuesto fallo confiesan que querían pasárselo bien y sin pruebas, afirmaron que podrían ejecutar código y que conocían muchas otras vulnerabilidades no reveladas. **Pura fanfarronería**. Snyder, jefa de seguridad de Mozilla, confirma que la denegación de servicio es reproducible en base a la información aportada por los dos bromistas, pero que no pueden confirmar la ejecución de código. Ocurre algo parecido a principios de agosto, cuando Jon "Johnny Cache" Ellch y David Maynor quisieron demostrar en una presentación en Black Hat cómo colarse en un Apple Macbook en 60 segundos a través de sus controladores "wireless". Finalmente todo resulta una gran exageración y la demostración, aunque vistosa, no era del todo real. En resumen, usaron otros controladores vulnerables que no pertenecían a Apple.

_ Microsoft **retira el galardón MVP a un programador que distribuía software espía**. MVP (Most Valued Professionals) es un reconocimiento anual que ofrece Microsoft a miembros destacados de comunidades que, de alguna forma, ayudan a mejorar productos Microsoft. Se basa en las contribuciones realizadas durante el año anterior y se nombran a través de un período de nominación. Tras reconocer que la aplicación por la que se le premiaba se distribuía junto con un programa espía, decide retirarle el premio a Cyril Paciullo (más conocido como Patchou) creador de Messenger Plus!. El programa viene integrado en su instalador con un "patrocinador" opcional que no es más que un simple malware espía.

_ **Oracle anuncia que mejora su sistema de notificación de alertas de seguridad**, añadiendo más información a la descripción de las vulnerabilidades. Esto responde a una aclamada demanda por parte de administradores de sus bases de datos, que sufrían desde hace años un confuso sistema trimestral de parches y kilométricos boletines. Parece que Oracle acaba reconociendo que la forma en la que venía describiendo sus problemas de seguridad resultaba manifiestamente mejorable y decide rediseñar su sistema de boletines que hasta ahora venía siendo poco más que un jeroglífico. Para ello, se ayuda de CVSS (Common Vulnerability Scoring System), un estándar que gradúa la severidad de manera estricta a través de fórmulas establecidas. De esta forma los administradores conocerán de manera objetiva (a través de un número) la gravedad de los fallos. CVSS es un sistema ya usado por compañías como Cisco, Qualys, Nessus y Skype que basa el cálculo de rango de criticidad en tres puntuaciones: Base (a su vez calculada a través de siete factores), temporal (un valor calculado a partir de tres factores) y ambiental (a través de dos). De estos tres factores principales, los dos últimos (temporal y ambiental) pueden modificar y corregir el primero (la puntuación base) según las circunstancias volátiles de la vulnerabilidad. Un sistema riguroso y objetivo que espera convertirse en el estándar de calificación de vulnerabilidades.

_ En octubre se introducen **más y mejores novedades en VirusTotal** para hacer frente a la creciente carga de trabajo que viene soportando. Aunque a nivel visualización de resultados los usuarios no notan nada nuevo, sí percibirán que los tiempos de espera para las peticiones se reducen de forma sensible respecto a lo experimentado en los últimos meses. En un periódico económico a nivel nacional, y ante la noticia de la mejora en VirusTotal, deciden que nuestros laboratorios son así:



Las amenazas informáticas pueden causar serios disgustos a las empresas. / AP

Hispasec amplía su laboratorio antivirus

EMPRESAS Todos los peligros que acechan desde la Red son bienvenidos en el área de investigación de la firma, que los analiza para ofrecer soluciones a sus clientes. Su capacidad va a triplicarse con un nuevo proyecto de I+D.

_ **Alan Cox**, un respetado desarrollador del núcleo de Linux y actual trabajador de Red Hat, se queja de la autocomplacencia del mundo del código abierto con respecto a la seguridad. Advierte de que mucho código abierto está lejos de ser seguro. "Lo que aparece en los medios de comunicación como que el código abierto es seguro y más fiable y que tiene menos fallos son afirmaciones muy peligrosas", dice Cox. "Un análisis de 150 proyectos de SourceForge (un repositorio de software de código abierto) no obtendría los mismos buenos resultados que el núcleo de Linux. La alta calidad sólo se aplica a algunos proyectos, los que tienen buenos autores y buenas revisiones de código". Alan Cox continua: "El debate de Microsoft diciendo "Mira qué seguros somos" contra Linux afirmando "Nosotros somos más seguros" no se está enfocando en los puntos importantes".

LMH, otro investigador relacionado con el proyecto Metasploit, pone en marcha en noviembre la iniciativa **"Month of the kernel bugs"**. La idea es publicar un nuevo error en el kernel de cualquier sistema operativo durante todos los días de noviembre. El objetivo es mostrar herramientas y procedimientos que ayuden a mejorar la calidad de los núcleos de cualquier sistema operativo. Una de las herramientas usadas para detectar estos errores es fsfuzzer, un programa capaz de encontrar fallos en una gran cantidad de sistemas de ficheros, además de otras herramientas destinadas a tantear los límites del software y que se desarrollan dentro del proyecto Metasploit.

Finalmente, se descubren: Once fallos en la rama 2.6.x de Linux, la mayoría relacionados con el montaje de sistemas de ficheros. Dos fallos en el núcleo de FreeBSD, ambos al montar sistemas de ficheros UFS. Un fallo en Solaris 10, también al montar sistemas de ficheros UFS. Ocho fallos en Mac OS X. Entre ellos un grave problema en DMG, formato muy común de instalación en entornos Mac. Tres fallos en controladores NetGear, dos de ellos permitirían la ejecución de código arbitrario a nivel de kernel. Un fallo en controladores D-Link, que permitía potencialmente la ejecución de código. Un fallo en Microsoft Windows, que permitiría provocar una denegación de servicio (pantallazo azul) o escalar privilegios a través de GDI . Dos fallos en Apple Airport, y un fallo en controladores inalámbricos de Broadcom. Este es el que causa más revuelo. El controlador de dispositivo inalámbrico Broadcom (BCMWL5.SYS) es vulnerable a un desbordamiento de memoria intermedia basado en pila que permite la ejecución de código arbitrario en modo núcleo. Se proporciona unido a los sistemas de muchos fabricantes y el fallo, con exploit público, puede ser aprovechado sin interacción por parte del usuario. Para colmo, es complicado delimitar la responsabilidad de publicar un parche.

_ El noviembre, los creadores de malware aprovechan de nuevo la credibilidad de una página consolidada para intentar infectar a usuarios de sistemas Windows. En la **Wikipedia alemana** se inserta un artículo fraudulento sobre el famoso gusano Blaster que enlazaba a la descarga de un malware que pretende ser una solución para una ficticia nueva variante.

_ Bernardo Quintero descubre sin querer una pequeña **denegación de servicio en Opera 9.02** bajo Windows (navegador al que se aficiona tras la insistencia de Sergio de los Santos). Al visitar la dirección “http:///”, se provoca una denegación de servicio que consume los recursos del procesador. Sería solucionado poco después por los programadores del navegador.

_ Cesar Cerrudo emprende una nueva campaña centrada en un solo producto: **La semana de los bugs en Oracle** (“Week of Oracle Database Bugs”), anunciada para principios de diciembre. La WoODB pretende centrarse en la publicación de una vulnerabilidad o error por día durante una semana, caracterizadas por no tener solución oficial y ser desconocidas hasta el momento. Su creador indica que bien podrían hacer “el año de los fallos en Oracle” sin ningún problema. Añade que incluso la compañía miente sobre sus esfuerzos de seguridad. Después de alguna que otra polémica, y por intereses no desvelados de forma clara, Cerrudo abandonaría la iniciativa poco después sin llevarla a cabo. Meses más tarde publicaría otras vulnerabilidades para Oracle en conferencias.



_ Hispasec detecta un **phishing a Banesto con intento de protección anti-inyección**. Una de las medidas de reacción contra un phishing, además de la obvia de cerrar el sitio o retirar las páginas, es inyectar basura en el formulario. La idea es dificultar a los atacantes el poder discernir entre los datos de víctimas reales y los falsos introducidos por una herramienta automática. Se observa el primer phishing que se vale de un CAPTCHA para evitar el envenenamiento del canal con basura, y solo obtener datos verdaderos de víctimas.

_ A finales de noviembre se descubre una **vulnerabilidad en GnuPG calificada de “obvia”**. Puede ser aprovechada por atacantes para ejecutar código arbitrario en el sistema afectado. El descubridor califica el problema de “obvio”, por lo que no se explica que lleve ahí desde hace casi 8 años.

A finales de 2006, **Inteco (Instituto Nacional de Tecnologías de la Comunicación)** comienza el estudio sobre la incidencia y confianza de los usuarios de Internet españoles. Se basa en la medición mensual de la frecuencia de los episodios de riesgo individual en una muestra amplia de más de 3.000 hogares panelizados online. Básicamente, los usuarios instalan voluntariamente un cliente que detecta el potencial malware en el sistema, contrastado contra la base de datos de VirusTotal. **Hispasec** es la encargada de desarrollar específicamente para este estudio la herramienta iScan, basada en microfirmas y consultas online a través de Internet para la identificación de malware. Se trata de la primera solución que hace uso del **“cloud computing”** en la detección de malware. Esta técnica que popularizaría en 2008 de la mano de algunas casas antivirus, aunque fue desarrollada sin ser conscientes de que el concepto sería tan popular dos años después. Pocos meses después, el estudio concluiría que el 70% de los ordenadores domésticos contiene malware o programas espía.



ELPAÍS.com | Tecnología — Miércoles, 30/1/2008, 09:27 h

Inicio | Internacional | España | Deportes | Economía | Tecnología | Cultura | Gente y TV | Sociedad | Opinión | Blogs | Participa | buscar

Ciberpaís | Meristation

ELPAIS.com > Tecnología

REPORTAJE

El 70% de los ordenadores domésticos contiene virus o programas espía

Más de la mitad del 'malware' detectado es de alto riesgo porque puede dañar los equipos o derivar en un engaño o fraude

RAMÓN MUÑOZ - Madrid - 13/05/2007

El estudio muestra, por primera vez, los hábitos que afectan a la seguridad en Internet: equipamiento de seguridad en los hogares, las medidas que los usuarios toman antes y después de las incidencias y la percepción relativa a la seguridad en Internet existente en los hogares españoles Refleja también la creciente exigencia por parte de los usuarios a las administraciones públicas de que "hagan de Internet un lugar seguro".

Una al día

22/01/2006 250.000 máquinas "zombies" al día en diciembre

Según un estudio que podemos ver en technewsworld.com, en el último mes se han batido todas las marcas. En diciembre, hasta 250.000 ordenadores al día han sido infectados por algún tipo de troyano que permitía controlarlos. Hasta siete millones y medio de "zombies" ese mes al servicio de spammers, phishers, virus, y demás indeseables de Internet.

250.000 "zombies" al día supone un incremento de un 50% respecto al mes anterior, lo que no es poco. Por países, estos sistemas se distribuyen así:

China: 17.10 %
Estados Unidos de América: 14.75 %
Alemania: 8.57 %
Francia: 5.61 %
España: 4.37 %
Corea: 4.35 %
Brasil: 4.06 %
Polonia: 4.05 %
Japón: 3.92 %
Reino Unido: 3.32 %

En números, nos da una cifra de aproximadamente 330.000 ordenadores secuestrados en diciembre en España. En este repunte de cifras a final de año, sin duda, han tenido mucho que ver las últimas variantes de Sober y la vulnerabilidad WMF de Microsoft Windows como causantes del robo de estas máquinas.

De la intención del reclutamiento masivo de ordenadores ya se ha hablado en una-al-día anteriormente. Con la debida coordinación, un sólo "click" del programa maestro permite ordenar a una red de miles de máquinas ejecutar una misma orden de ataque. La mayoría de usuarios ni siquiera conoce la clandestina actividad de su sistema y en un principio, simplemente suelen percibir cierta merma en su velocidad de navegación y proceso. Las máquinas "zombie" se aglutinan en los denominados "botnets", anglicismo que se refiere a la asociación en red (nets) de máquinas autónomas (bots, apócope del término sajón robots). Los "botnets" pueden concentrar un gran número de máquinas "zombie" que se coordinan para gestionar el envío de correo basura, pero, sobre todo, suelen ser las culpables de los ataques de denegación de servicio distribuido (DDoS).

Hace ahora justo un año, se publicaba un estudio de Honeynet.org, especialistas en el seguimiento de redes automatizadas de máquinas comprometidas, efectuado entre noviembre de 2004 y enero de 2005. En él se monitorizaron más de 100 "botnets" diferenciados, alguno de ellos con más de 50.000 máquinas "zombie" comprometidas. Se llegaron a censar más de 226.000 direcciones IP distintas por canal auditado, lo que nos ofrece una idea aproximada de la magnitud del problema. Un año después, se bate récord de máquinas infectadas diariamente.

¿Qué potencia se puede alcanzar con tal ejército de máquinas? La computación coordinada es muy importante y no siempre se utiliza con fines despreciables. Según lo que se ha podido conseguir con muchas menos de esas 250.000 máquinas "zombies" identificadas diariamente en diciembre, podremos llegar a hacernos una idea del problema que supone para la seguridad que ciertos irresponsables controlen a su antojo tal cantidad de sistemas, cada uno con su capacidad de proceso y con su ancho de banda dispuestos a ser sacrificados a la primera orden.

Un ejemplo de computación coordinada es Distributed.net, un proyecto destinado a comprobar la seguridad de los algoritmos de cifrado más conocidos. Voluntarios prestan de forma altruista los tiempos "ociosos" de sus máquinas para procesar datos del algoritmo de cifrado elegido. Mediante un sistema distribuido donde son asignados bloques de claves a cada cliente y coordinadas con un servidor, se intenta por fuerza bruta averiguar el mensaje cifrado con un algoritmo concreto.

En 1999 se propusieron romper un mensaje cifrado con el algoritmo RC5 de 64 bits por fuerza bruta y les llevó casi cuatro años probar 15.769.938.165.961.326.592 claves para finalmente descubrirla en julio de 2002. Desde diciembre de ese mismo año intentan, insistentemente, descifrar un mensaje cifrado ahora con RC5 de72. bits, lo que implica probar 2 elevado a 72 claves, un número de 22 cifras. Para el primer desafío contaron "sólo" con 331.252 máquinas de todo tipo durante todo el proceso. Para el desafío actual todavía no resuelto, han participado ya 69.212 ordenadores.

SETI, o la Búsqueda de Inteligencia ExtraTerrestre, es un esfuerzo científico que trata de determinar si hay vida inteligente en el Universo. Su proyecto más exitoso es SETI@Home, al igual de Distributed.net, utiliza sistemas personales conectados a Internet para analizar la increíble cantidad de información que el equipo SETI recibe en sus radiotelescopios. Las señales de "ruido" del Universo recibidas, son codificadas y enviadas por paquetes al cliente. Este es un pequeño programa que cada usuario mantiene voluntariamente instalado en su sistema. Aprovecha los tiempos muertos para analizar y procesar los paquetes y son devueltos al equipo SETI con los resultados. La probabilidad de que un ordenador detecte el murmullo lejano de una civilización extraterrestre es mínima, pero con tal capacidad de computación unida, las posibilidades aumentan.

Seti@Home cuenta actualmente con unos 370.000 usuarios registrados, y unas 750.000 máquinas en todo el mundo. En España, menos de 9.000. En este caso, teniendo en cuenta los 330.000 "zombies" detectados en nuestro país en diciembre, son más las máquinas que tienen programas instalados clandestina e involuntariamente que de forma consciente, y mayores los recursos invertidos para fines ilegales y prohibidos que para proyectos interesantes y altruistas.

La intensidad de los ataques perpetrados por redes "zombies" o "botnets", es poco menos que incontenible. Unir de forma coordinada la capacidad de proceso y "bombardeo" de cada máquina, puntando su caudal hacia un objetivo fijo y determinado, puede terminar por consumir los recursos de las redes más anchas y preparadas. Si estas redes de "zombies" se emplean, además, para el envío de correo basura, el resultado es el que podemos comprobar cada día en las casillas de correo de todos los usuarios del planeta: miles de millones de mensajes inútiles que se cuelan en nuestros clientes, (más los miles de millones ya desechados

por los programas anti-spam), además del phishing y de los correos infectados por virus. En gran parte, es culpa de estos “zombies” tal cantidad de basura desproporcionada, y, para colmo, hoy por hoy según estos nuevos datos, los sufrimos más que nunca.

Sergio de los Santos

22/02/2006 Manzanas y gusanos

Se habla en los medios de un par de virus (o troyanos o gusanos) que han sido detectados replicándose a sí mismos. Esto no sería en absoluto novedad, sino fuera porque el código infecta a los MAC OS X de Apple.

¿Está siendo atacado el sistema operativo más elegante? No es un ataque propiamente dicho y a uno de ellos, incluso, ni siquiera se le puede llamar virus. Por ahora los usuarios de Mac pueden respirar tranquilos: los virus de difusión masiva siguen siendo una parcela reservada para Microsoft y Windows, pero quizás se debería reflexionar sobre esta posibilidad en un futuro.

El día 13 de febrero, un usuario anónimo (no podía ser de otra forma) dejaba un mensaje en uno de los foros más populares para usuarios de Mac, MacRumors. En él se ofrecía a través de un enlace a un servidor externo, un archivo comprimido que se supone contenía imágenes de la nueva versión de Mac (la OS X 10.5, llamada Leopard). El fichero se llama latestpics.tgz y con él, llegó la polémica.

Aunque lo aparentase, no contenía imágenes. Eran simples ejecutables UNIX compilados y camuflados... un programa. A partir de aquí, podríamos calificar a este engendro de troyano, por ocultarse como algo que realmente no era. Estas denominaciones han provocado profundas discusiones, pues las connotaciones implícitas que conlleva calificar de troyano a un código no son las mismas que calificarlo de virus o gusano.

Esta última nomenclatura denota más vulnerabilidad por parte del sistema operativo (virus y gusanos pueden ejecutarse con mínima interacción del usuario, a escondidas, y pueden replicarse hábilmente entre los sistemas) mientras que un troyano es habitualmente ejecutado consciente o inconscientemente por un usuario, lo que deja caer la balanza de la culpa y la responsabilidad más hacia este último. Los defensores de Mac, en este punto, quieren dejar muy claro que el sistema operativo es seguro, pero no puede hacerse responsables de las intenciones o consecuencias de la utilización por parte de un usuario incauto e irresponsable.

Al archivo, una vez analizado se le podían reconocer rutinas destinadas a autorreplicarse e infectar otros sistemas Mac. Aprovechaba la lista de contactos de iChat para enviarse a sí mismo e intentar contagiar a otros usuarios. Sobre esto, los usuarios de Mac han rechazado igualmente la denominación de “virus”, pues necesita de bastantes acciones irresponsables por aparte del usuario para poder replicarse. En primer lugar el usuario de iChat debe aceptar la transferencia de las supuestas imágenes, descomprimirlas y ejecutar el archivo en su interior. Si el usuario pertenece al grupo de administradores se infectará, si no, el sistema operativo le pedirá las credenciales porque el malware intenta escribir en zonas reservadas. Esto es como en cualquier otro sistema operativo, aunque entre usuarios Mac sea más habitual relegar la cuenta de root a labores administrativas. Necesitar de tanta ayuda para infectar, debilita enormemente las posibilidades de contagio masivo.

Parece ser que también es capaz de infectar otros archivos en el sistema, aunque su código no resulte

demasiado sofisticado. Además, cabe destacar que no aprovecha ninguna vulnerabilidad conocida o desconocida del sistema para ejecutarse. Su “modus operandi” para infectar un sistema que lo aloje, resulta completamente manual.

En todo caso, el código ha llegado al estatus de malware, pues varias casas antivirus lo han incluido en sus firmas bajo el nombre de OSX/Leap (otros como OSX/Oomp-A), cosa que no ocurre a menudo aunque, a tenor de lo acontecido estos últimos días, cabría preguntarse si está cambiando esta tendencia. Sólo una semana después de la aparición de este troyano, se hacía público la existencia de un segundo código indeseado para Mac OS X. Igual de minoritario (puede ser considerado una prueba de concepto), Inqtana-A sí puede ser llamado virus pues aprovecha una vulnerabilidad en el componente Bluetooth de este sistema operativo para ejecutarse y, teóricamente, la necesidad de una mano que lo ejecute es mínima. Se replica de sistema vulnerable a sistema vulnerable a través de Bluetooth, pero es casi seguro que encuentre pocos huéspedes que puedan alojarlo, pues Apple publicó un parche para ese problema en mayo de 2005, con lo que la mayoría de sistemas hoy día serán inmunes.

Los usuarios de Mac han permanecido durante muchos años ajenos a la amenaza del malware, son confiados y la historia les avala. Desde que en 1982 apareciese Elk Cloner (creado por un quinceañero) e infectase a sistemas Apple II (nada que ver con los Mac OS X actuales) a través de disquetes, pocas han sido las oportunidades de bautizar a un virus. El problema es que en dos semanas, han tenido que hacerlo en dos ocasiones.

Aunque Mac OS X es un excelente sistema operativo, seguro por diseño, son siempre los usuarios que manejan cualquier máquina los que pueden resultar realmente peligrosos. Si no ejecutan código no confiable y se mantienen actualizados, no sufrirán a estos dos nuevos especímenes encontrados. Aun así, no conviene bajar la guardia ante posibles amenazas futuras más sofisticadas y propagadas que ocurrirán, según las tendencias actuales, sólo y exclusivamente cuando la creación de malware para este sistema operativo proporcione algún tipo de rentabilidad significativa a sus creadores.

De hecho, de una encuesta promocionada por Sophos sobre 600 usuarios, el 79% pensaba que Apple será objetivo del malware en el futuro, aunque la mitad pensara que nunca llegaría a suponer el problema que representa para usuarios de Microsoft. Lo curioso de la encuesta, quizás, es ese 21% que se muestra confiado y no cree que el malware vaya a suponer nunca un problema para su sistema operativo.

Esa confianza, se use el sistema operativo que se use, resulta mala compañera y es bastante probable que haya impulsado, por ejemplo, a muchos usuarios de Mac a ejecutar alegremente las supuestas y esperadas imágenes del nuevo sistema operativo, sin preguntarse si eran realmente imágenes, quién las enviaba y por qué. Esta prudencia básica, por experiencia, es algo que ya muchos usuarios de Windows se plantean antes de lanzar su ratón sobre archivos desconocidos, mientras que a usuarios de Mac, también por propia experiencia, es probable que ni se les pase por la cabeza.

Además de este debate abierto sobre el futuro del malware para Mac, habrá que estar atento al potencial impacto que tendrá en la seguridad la posibilidad de ejecutar el sistema operativo bajo microprocesadores Intel.

Sergio de los Santos

28/03/2006 Troyanos bancarios: nuevos enfoques contra sistemas de seguridad

Que el asunto de los troyanos orientados al fraude bancario se está poniendo muy serio es algo que podemos comprobar en Hispasec día a día en nuestro servicio VirusTotal. Son literalmente cientos los que son analizados en el servicio cada día, y esta legión no está formada sólo por variantes de las familias ya clásicas (Bifrose, Goldun, Zagaban, Psyme, etc.) sino también por nuevos ejemplares que se suman a las filas de esta amenaza creciente.

Los códigos TAN (Transaction Authentication Number, Número de Autenticación de Transacción para los hispanoparlantes) son utilizados por algunas entidades bancarias como una forma para reforzar la seguridad a la hora de realizar operaciones desde las cuentas online. Básicamente se trata de claves de un solo uso que el usuario puede recibir de su entidad bancaria por ejemplo vía SMS (una vez por código) o por correo ordinario (una lista para varios usos). Teóricamente, este mecanismo de 'doble autenticación' ofrece una protección mayor que el uso de una clave de autenticación inicial con el banco más el uso típico de una secundaria para realizar operaciones.

Sin embargo, y como es natural, los desarrolladores de malware van modificando sus criaturas para adaptarse a nuevos retos. Otro representante de las anteriormente nombradas familias clásicas de troyanos, con denominación Kaspersky Trojan-Spy.Win32.Goldun.im, ha optado por añadir a sus múltiples capacidades (entre las que se encuentra funcionalidad rootkit para ocultarse convenientemente en el sistema) la captura de estos códigos de transacción para poder realizar sus actividades fraudulentas.

Este ejemplar utiliza un sistema sencillo man-in-the-middle, pero que si es convenientemente explotado, puede ser sumamente eficiente: interceptando la comunicación HTTPS con las entidades afectadas (en este caso dos bancos alemanes: Postbank y Deutsche Bank), captura el TAN que envía el usuario y seguidamente muestra un mensaje de error a la víctima. Mientras ésta se pregunta que demonios ha pasado, llega para el atacante el momento de hacer rápido uso de dicho TAN para poder acceder a la cuenta de la víctima, dado el periodo de vida limitado que tiene dicho código de transacciones.

Visto de forma global, en realidad este ejemplar de malware no constituye ninguna novedad técnica, pero pone de nuevo en evidencia que ningún sistema de protección es infalible a lo largo del tiempo contra la cada vez más agresiva acción de este tipo de amenazas.

Como de costumbre, ante este tipo de actividades lo recomendable es seguir al menos unas cuantas directrices técnicas, como mantener convenientemente parcheado el sistema operativo, usar un buen antivirus y un igualmente competente firewall personal. Sin embargo, lo más importante es aplicar el sentido común, sobre todo en lo referente a los hábitos de navegación y al tratar con el correo electrónico.

Julio Canto

24/04/2006 Sexo, troyanos, y phishing

Ya lo decía Nietzsche, "el sexo es una trampa de la naturaleza para no extinguirse". Ahora son los phishers los que están utilizando esta trampa como reclamo para infectar a los usuarios con troyanos y capturar sus claves de acceso a la banca electrónica.

El phishing tradicional se presenta en forma de correo electrónico simulando provenir de la empresa

suplantada, la mayoría de las veces una entidad financiera, e instando al usuario con cualquier excusa a introducir sus claves en un formulario que realmente envía los datos al phisher.

Aunque simple, llega a ser efectivo. El hecho de que continúen con esa estrategia lo demuestra por si sólo, sin necesidad de contar con estadísticas o datos concretos de incidentes reales, tema tabú por otro lado. Dejando claro que el phishing tradicional es un tema importante, que mueve mucho dinero, no es menos cierto que en muchas ocasiones es más el ruido que las nueces. Ruido que suele traducirse en daño a la imagen corporativa, publicidad negativa difícil de cuantificar, si bien no son pocas las veces que ese efecto colateral supera a la pérdida directa del ataque, ya que el phisher no obtiene ningún resultado.

Por una causa u otra, en ocasiones por ambas, el phishing tradicional es sin duda temido y bien conocido. Sin embargo, pese a su popularidad, no es ni el único ni, tal vez, el método más efectivo de ataque que utilizan los phishers. Existe una amenaza oculta, casi fantasma, de la que apenas se tienen datos globales, y que lleva ya tiempo siendo explotada de forma efectiva por los phishers: troyanos.

A diferencia del phishing tradicional, los troyanos permiten diversidad de ataques una vez la máquina del usuario está comprometida. El phishing tradicional es efectivo en el caso de contraseñas estáticas, requiere que el usuario se crea que el e-mail fraudulento proviene de su banco, y que meta las claves en una página cuya dirección no corresponde a la web de su entidad. Amén de que son rápidamente detectados y su desactivación varía entre pocas horas y, en el peor de los casos, algunos días.

Por su parte, los troyanos pasan mucho más desapercibidos y pueden capturar los datos sin levantar sospechas al usuario, no necesitan exponerse al conocimiento público a través de un spam, y su esperanza de vida es mucho mayor, suelen descubrirse semanas o meses después de haber iniciado su actividad.

Además, los troyanos no tienen las limitaciones de una página web falsa y pueden burlar las protecciones más habituales. Un troyano puede capturar tanto las pulsaciones de teclado, como pequeñas áreas de pantalla alrededor del cursor en el caso de teclados virtuales, o capturar los datos del formulario en claro, antes de que el navegador lo pase por SSL. Pueden modificar las páginas que la web del banco presenta al usuario, o los datos que el usuario envía al servidor seguro de la entidad, llevar a cabo ataques tipo hombre en medio, vulnerar los sistemas basados en clave única, tokens, SMS, DNI electrónico, etc.

Una vez una máquina está comprometida, no se puede garantizar la seguridad de una transacción realizada a través de ella.

En el laboratorio de Hispasec llegamos a analizar más de 50 muestras diarias distintas de troyanos bancarios, que son enviadas al servicio VirusTotal. Distinguimos principalmente dos escuelas, internamente las denominamos rusa y brasileña, que difieren bastante en la estrategia, técnicas utilizadas, y programación.

Si bien, además del fin común que persiguen (robar claves de acceso a la banca electrónica), hemos encontrado otro punto en común que suele aparecer con asiduidad en ambas escuelas: el sexo como reclamo para infectar usuarios.

El sexo es un tema utilizado recurrentemente en ingeniería social (término utilizado en seguridad informática a las técnicas para engañar al usuario), así como otras temáticas mucho más románticas. No olvidemos el famoso “iloveyou”, gusano que hiciera aparición en mayo de 2000, y que se propagó por todo el mundo gracias a que pocos se resistieron a abrir una supuesta carta de amor que llegaba a su buzón de correo.

En el caso de los troyanos bancarios que nos ocupa las temáticas suelen ser menos románticas y más explícitas. Pueden llegar adjuntos en un e-mail como una supuesta foto algo subida de tono, hasta ahora siempre de una fémina, o un mensaje, tipo spam, que nos invita a visitar una página con contenidos para adultos.

En ambos casos, y como norma general, el usuario logra visualizar el contenido que esperaba, lo que minimiza las sospechas de que algo irregular ha ocurrido.

En el caso de los adjuntos el archivo suele ser un ejecutable, con la extensión real ofuscada y que aparece representado en Windows con el icono utiliza para los formatos gráficos. Al ser abierto el ejecutable muestra la esperada foto, pero al mismo tiempo que el usuario se recrea en su visualización, de forma oculta, el troyano es instalado en su sistema.

En la otra variante ampliamente utilizada, la del mensaje que incita al usuario a visitar una página, también se muestran los contenidos adultos. En esta ocasión la página web suele incluir además algún exploit que aprovecha vulnerabilidades conocidas del navegador, la mayoría de veces contra Internet Explorer por ser el que mayor cuota de mercado tiene y por tanto, a priori, augura mayor número de infecciones al atacante.

En el caso de que el usuario no mantenga su sistema actualizado con los últimos parches de seguridad, el troyano es descargado e instalado en su sistema de forma oculta mientras visualiza el contenido adulto.

Algunos ejemplos de los contenidos utilizados por los últimos troyanos pueden encontrarse en:
http://blog.hispasec.com/laboratorio/118

Las recomendaciones para prevenir este tipo de infecciones son básicas, por un lado debemos ignorar todos los mensajes de spam, no abrir sus archivos adjuntos ni visitar sus enlaces, directamente borrarlos. Las soluciones antispam también minimizarán el riesgo de recibir este tipo de mensajes.

Por otro lado es fundamental que mantengamos el sistema operativo puntualmente actualizado con los últimos parches de seguridad. Especial atención a disponer de la última versión de nuestro navegador. En el caso de Windows, sistema al que de momento se dirigen este tipo de troyanos, se recomienda activar las actualizaciones automáticas y/o visitar periódicamente el sitio http://windowsupdate.microsoft.com

Un buen antivirus también será de gran ayuda para prevenir estas vías de infección y otras estrategias de distribución seguidas por los troyanos bancarios y el resto del malware.

Como hemos visto, en el terreno virtual también es necesario tomar una serie de precauciones para disfrutar del sexo de forma segura. Por terminar como empezamos, con una cita, debemos ser más críticos con lo que nos ofrecen en Internet y no dejarse ofuscar como Woody Allen, que llegó a decir, "Solo existen dos cosas importantes en la vida. La primera es el sexo y la segunda no me acuerdo".

Bernardo Quintero

12/07/2006 Troyanos bancarios y evolución del phishing

El phishing tradicional, aquel que llega a través de e-mail y nos invita a visitar una página web que imita a

la original de la entidad para que suministremos las claves de acceso, ya no es el principal vector de ataque del fraude en Internet. El número de troyanos bancarios supera en número y efectividad al phishing más conocido, sin embargo no hay datos públicos sobre su actividad ni modus operandi. A continuación mostraremos un vídeo de como actúa uno de esos troyanos que lleva meses entre nosotros.

El phishing tradicional

El phishing tradicional es fácil de advertir, ya que es enviado de forma masiva a nuestros buzones de correo, lo que facilita su localización temprana y los avisos relativos a casos concretos. A la parte pública, con iniciativas de información y alerta o las recomendaciones de seguridad publicadas por las propias entidades financieras, hay que sumar las acciones privadas entre entidades y empresas de seguridad que permiten la detección de sitios fraudulentos antes que sean conocidos. En estos últimos casos los incidentes no suelen trascender, por lo que el número de ataques phishing es mayor que el que pueda revelar cualquier estadística pública.

Además de la detección, más o menos temprana, otro apartado importante es el de la mitigación. El phishing tradicional ofrece oportunidades al usuario para que pueda diferenciar el sitio original de uno fraudulento, ya que hay elementos visibles que permiten su identificación.

En la mayoría de los casos, el usuario podrá observar que la URL o dirección que aparece en el navegador no corresponde con la de su entidad, o que la conexión no es segura (no aparece el https ni el candadito en el navegador). Y como medida preventiva, por activa y por pasiva, se le está recomendando a los usuarios que deben hacer caso omiso de los mensajes de correo electrónico que le piden que introduzca su usuario y contraseña con cualquier excusa.

Las entidades y empresas de seguridad también tienen fácil prevenir ciertas prácticas de phishing tradicional, mitigar la funcionalidad de los que se detecten activos y cerrarlos de forma rápida.

Pese a que efectivamente el phishing tradicional es bastante primitivo, no deja de ser un problema importante. Aunque el número de incidentes reales es prácticamente un tema tabú, nunca se ofrecerán datos de usuarios afectados o cantidades económicas concretas, el hecho de que no decaigan los ataques es la mayor constatación de que sigue siendo una actividad rentable para los estafadores.

El problema no acaba en el fraude en sí mismo, a los ataques con éxito que puedan darse hay que sumar la imagen negativa que afecta a entidades con nombre propio y al canal en general, efecto colateral que en ocasiones es más perjudicial para las entidades que el propio fraude directo.

En este contexto, cuando aun no hemos superado el phishing tradicional y los diferentes agentes implicados discuten sobre responsabilidades o estrategias para luchar contra este tipo de estafas, existe una evolución del phishing que es más desconocida y complicada de prevenir.

Los troyanos bancarios

Aunque todo el mundo ha escuchado hablar de los troyanos bancarios, no existen datos concretos sobre su proliferación ni sobre los métodos que utilizan.

Por norma general los troyanos bancarios suelen asociarse a los keyloggers, programan que capturan las pulsaciones de teclas cuando introducimos nuestras claves. Incluso en círculos más especializados se tiene esa errónea percepción, basta con observar como las propias entidades implantan teclados virtuales en

un intento de prevenir su acción.

La realidad es que ya hace tiempo que la técnica tipo keylogger dejó de ser la utilizada mayoritariamente por los troyanos bancarios, precisamente por la proliferación de teclados virtuales. Hoy día los troyanos bancarios capturan las contraseñas de manera independiente a si se introducen las claves por el teclado real o por un teclado virtual, por mucho que este último se mueva o cambie la posición de las teclas.

A continuación vamos a mostrar un vídeo de un troyano bancario que lleva a cabo su acción pese a que el usuario sigue recomendaciones de seguridad tales como escribir directamente la dirección, comprobar el https, o el certificado de la entidad.

http://www.hispasec.com/directorio/laboratorio/phishing/demo3/troyano_banesto.htm

No se trata de un troyano especialmente avanzado ni novedoso, lleva meses actuando en España, protagonizando incidentes reales, y es bien conocido entre las propias entidades y antivirus. Sin embargo aparecen variantes a razón de una por semana prácticamente, todas ellas enfocadas a varias entidades españolas e internacionales.

Lo más preocupante es que la evolución de este tipo de malware es constante. En el Laboratorio de Hispasec llevamos tiempo viendo, por ejemplo, troyanos que son efectivos contra el uso de certificados en los clientes, tokens y claves de un sólo uso, diferentes estrategias contra los sistemas de tarjetas de coordenadas, etc.

No estamos hablando de pruebas de concepto o troyanos de laboratorio, sino de especímenes reales que llevan ya tiempo infectando los sistemas y afectando a los usuarios. De estos troyanos, sólo una pequeña parte es analizada, y un porcentaje aun inferior de esos análisis llega a las entidades afectadas.

En estos momentos los laboratorios de las empresas antivirus están saturados por el volumen de malware en general que se produce, de forma que sólo puntualmente ofrecen datos concretos sobre algunos especímenes. No es un problema de los antivirus, es que a día de hoy es materialmente imposible analizar y publicar informes de todos los especímenes que aparecen.

Las entidades recurren a empresas de seguridad para que analicen algunos sistemas de usuarios comprometidos, pero el número de troyanos detectados con esta estrategia es ínfima, además de ser un esquema reactivo, inefectivo, muy poco escalable y menos rentable.

En VirusTotal estamos recibiendo más de 5.000 muestras diarias para analizar de forma automática, aproximadamente un 30% de ellas están relacionadas con el crimeware. En Hispasec analizamos "a mano" unos 90 troyanos bancarios diariamente, sólo para detectar a que entidades afectan y a donde van a parar los datos capturados.

El desconocimiento de este tipo de troyanos, las direcciones concretan a las que apuntan, o los métodos generales que utilizan para capturar las contraseñas, impiden a las entidades financieras actuar tanto de forma reactiva como preventiva contra ellos.

El problema del phishing no acaba aquí, seguirá evolucionando, lo que debe también evolucionar es la forma de abordarlo, ya que en la actualidad no se está llevando a cabo de forma efectiva, hay muchas áreas de oportunidad desaprovechadas.

Es fundamental que, ante la diversificación de las técnicas, exista una cooperación real y que los agentes implicados superen sus intereses particulares, de lo contrario nos seguirán ganando la partida.

En estos momentos, desde el propio sector de la seguridad, hay muchos intereses creados respecto a los sistemas de autenticación empleados. Sin embargo, el talón de Aquiles y principal caballo de batalla es y será la integridad del sistema del usuario.

En este terreno debemos sumar lo que tienen que ofrecernos (y debemos exigirles) las casas antivirus, hoy por hoy cuentan con el software de seguridad más implantado a nivel de usuario y con los recursos humanos más especializados a nivel técnico. Sin embargo suelen ser convidados de piedra en algunos grupos antiphishing.

Tampoco hay que olvidar la responsabilidad del sistema operativo o del navegador, ya que muchos ataques aprovechan vulnerabilidades o debilidades del software. Sumemos los ISPs, las fuerzas de seguridad, legislación, iniciatias específicas desde la administración pública, aportaciones de la comunidad académica, asociaciones de usuarios...

Luchar contra el phishing y las estafas en Internet de forma unilateral es condenarse al fracaso.

Bernardo Quintero

31/08/2006 La decadencia de los gusanos de infección masiva

Larry Seltzer publica en eWeek una reflexión sobre el escaso impacto actual de los gusanos de red. Si en otros tiempos fueron capaces de afectar a millones de usuarios de Windows (aunque también han existido para servidores PHP, por ejemplo), degradar redes mundiales y permanecer activos durante meses, hoy representan una simple reseña más en las firmas de antivirus. Sin embargo, esto no significa que los sistemas informáticos de consumo no estén en su peor momento en cuanto a niveles de infección.

Bajo el título "The end of the worm era" (el fin de la era de los gusanos), Seltzer comienza hablando sobre el virus W32.Wargbot que aprovecha la vulnerabilidad descrita en el boletín MS06-040 de Microsoft. Este virus ha pasado (o está pasando) sin pena ni gloria por los sistemas (especialmente Windows 2000) sin que haya causado un mayor destrozo. La vulnerabilidad dejaba la puerta abierta a la creación de un gusano y este no tardó en aparecer. Una simple conexión abierta a una red podía permitir el envío de paquetes manipulados y la ejecución de código arbitrario en todas las versiones de Windows.

Estos tipos de fallos de seguridad fueron los responsables de gusanos tan efectivos como el infame Blaster, que se alimentaba de la vulnerabilidad descrita en MS03-039. Sasser, meses después, apareció también a principios de 2004 con un método muy parecido. Ambos causaron estragos en redes de todo el mundo, y millones de personas observaban impotentes cómo les aparecía el mensaje de que había ocurrido un fallo crítico y el ordenador se apagaría en un minuto.

Pero esto fue hace tres años, y quizás fuimos testigos del último de los grandes gusanos de expansión e infección masiva. Hoy no es lo habitual, y la discreta presencia de Wargbot lo confirma. Esto no quiere decir que la amenaza sea menor, simplemente que la tendencia cambia. Las primeras versiones de Blaster eran un desastre en cuestión de programación, y aun así consiguió una propagación masiva. Wargbot es mucho más sofisticado, y no habrá sido tan famoso, pero seguro que ha cumplido la misión para la que fue

creado y ha logrado que se lucren de alguna forma sus programadores. Si bien los gusanos pueden estar en decadencia, los troyanos bancarios campan a sus anchas en ordenadores de todo el mundo, y decenas de nuevas versiones aparecen cada día. Los niveles de infección siguen siendo excesivamente elevados, pero no precisamente por gusanos de gran expansión. Se busca la eficacia silenciosa de virus, troyanos y gusanos, huyendo de la infección masiva y del fácil reconocimiento de casas antivirus.

Las causas de esta decadencia de gusanos de red pueden ser muchas. La aparición del Service Pack 2 para Windows XP, con el cortafuegos activado por defecto, y su mejora de la seguridad en general, puede ser una de las más significativas. Un estudio realizado por Microsoft, revela que del total de sistemas que ha desinfectado su "Malicious Software Removal Tool" sólo un 3% corresponde a XP SP2, mientras que XP y XP SP1 acumulan el 63% de las infecciones detectadas.

Las actualizaciones automáticas también ayudan a mitigar el impacto de estos gusanos, previniendo a los usuarios de infecciones causadas por vulnerabilidades. Sobre este punto (y de lo que no habla Seltzer) es interesante destacar lo "contraproducente" de una actividad vírica masiva y descontrolada que aprovecha agujeros de seguridad. Cada vez son más rápidos en aparecer los virus y gusanos que aprovechan vulnerabilidades críticas, y esto ha podido provocar una especie de muerte por éxito del sistema de infección masivo. Los usuarios ajenos a la seguridad, que no parchean sus sistemas, comprueban como el ordenador se vuelve ya no sólo lento e inestable, sino absolutamente inoperativo al poco tiempo. Esto comenzó a constatarse durante 2004, cuando era imposible conectar un ordenador con un Windows no parcheado a Internet, pues era cuestión de minutos que Blaster o Sasser aparecieran infectándolo todo y obligando a una instalación completa con parches incluidos.

Esto marcó un punto de inflexión, y el campo de la infección masiva por gusanos se ha visto tan saturado desde entonces, que literalmente es ya imposible mantener un ordenador "usable" durante un periodo de tiempo razonable si no es con un cortafuegos y con los parches de seguridad correspondientes. Prácticamente han sido los propios gusanos los que han "obligado" sin remedio a los usuarios, incluso a los más descuidados y temerarios, a parchear un sistema y refugiarse detrás de un cortafuegos, y sin vulnerabilidades, no hay forma de propagarse. Quizás han cavado su propia tumba por un excesivo éxito. Sin embargo, la evolución sigue su camino y los niveles de infección siguen altos. Los troyanos bancarios, mucho más discretos y que encuentran principalmente en los navegadores la puerta de entrada en los sistemas operativos, han tomado el relevo y representan hoy una de las mayores amenazas víricas de las que preocuparse.

Sergio de los Santos

24/10/2006 Malware y phishing, ¿ponemos más puertas al campo?

Los sistemas de seguridad reactivos, basados en firmas tradicionales para el malware y listas negras para el phishing, están obsoletos y se muestran insuficientes para abordar una realidad cuyos números y efectos se desconocen.

La Real Academia Española describe "poner puertas al campo" como frase coloquial usada para dar a entender la imposibilidad de poner límites a lo que no los admite.

Por definición, tanto el malware como el phishing son conjuntos finitos, si bien están en continuo crecimiento. La producción actual es tan prolífica que a efectos prácticos es imposible luchar de forma

efectiva intentando poner una nueva “puerta” para cerrar la vía de entrada de cada nuevo caso de malware o phishing.

¿Se desconoce la magnitud del problema?

Cuando uno trabaja dentro del sector tiene acceso a material de primera mano y tendencia a perder la perspectiva que se distingue del problema desde el exterior. Es normal que difiera la percepción de un usuario respecto a un profesional de la seguridad.

Tener puntos de vistas diferentes suele ser complementario y enriquecedor. Además, tradicionalmente las casas de seguridad han realizado, en ocasiones o de forma puntual, un mal uso de las estadísticas y las alertas, utilizándolas como herramienta de marketing para provocar la necesidad de adquirir unos determinados productos. No es de extrañar que el usuario de hoy mantenga cierta actitud crítica, por otro lado recomendable, cuando se le habla de los peligros que acechan en Internet.

Ahora bien, cuando uno lee en prensa que aparecen 2.000 nuevos virus cada mes de boca de un reputado experto en seguridad, ya no es un simple problema de percepción entre usuarios finales y profesionales del sector. La brecha es mayor.

Algunos números

Un laboratorio antivirus puede recibir cada día una media de mil nuevas muestras de malware para las que su solución no disponía de firma de detección específica. No hay ninguna errata en los números, hablamos de 1.000 en 24 horas, Y hay casos donde el volumen es mayor.

El phishing y el robo de credenciales de acceso a banca, al contrario del malware, tal vez sea una actividad más visible. No en vano la estrategia más común por parte de los atacantes es realizar un spam masivo para hacer llegar la dirección falsa al mayor número de víctimas potenciales. Todos hemos recibido varios mensajes de ese tipo, y más o menos podemos hacernos una idea del volumen.

Ahora bien, cuando hablamos de troyanos bancarios o de phishing segmentado entramos en un terreno mucho más oscuro. Como dato, en el laboratorio de Hispasec analizamos más de 100 troyanos bancarios cada día.

¿En qué se traducen estos números?

La situación es algo contradictoria. Vivimos la época con mayor número de amenazas e incidentes en Internet, si bien la percepción general sobre la inseguridad se ha relajado respecto a años anteriores.

Algunos culpables

El malware ha dejado de ser noticia. Antes solía aparecer regularmente un gusano de propagación masiva que obtenía la atención de los medios tradicionales y protagonizaba titulares.

Ahora la estrategia de los atacantes ha cambiado. En vez de un gusano de propagación masiva que infecta miles de usuarios en poco tiempo, pero que también provoca que los antivirus reaccionen en tiempo récord, prefieren distribuir miles de variantes que infectan a más usuarios, pasan más desapercibidas, y dificultan la labor de detección de los antivirus.

Además el malware actual es menos perceptible por los usuarios infectados. Atrás quedaron los virus que mostraban efectos en las pantallas de los usuarios, eliminaban archivos, o los gusanos que provocaban un aumento en el tráfico de red. Los troyanos y el spyware, reyes indiscutibles de la escena actual, es software diseñado para permanecer oculto en los sistemas y no dar señales de su actividad.

La situación actual

A efectos prácticos, el disponer de un antivirus o no hacer caso a los mensajes de phishing no garantiza a un usuario que su sistema no esté infectado o sea víctima de una estafa. De hecho, es muy común encontrarse sistemas con antivirus instalados donde conviven varios troyanos y/o spyware. Con frecuencia los usuarios nunca llegan a ser conscientes de las infecciones, más de una vez habremos escuchado la frase: "parece que este Windows tiene demasiado tiempo, va muy lento y con errores, toca formatearlo de nuevo". Sí, en muchas ocasiones la responsabilidad no es del sistema de Microsoft (comodín para todos los males), o al menos no en exclusividad.

Tampoco faltan casos de usuarios que han sido víctimas de fraude a través de la banca electrónica por Internet que además de disponer de antivirus actualizado nunca han visitado una página de phishing.

Lo que hay que exigir

Los sistemas de seguridad totalmente reactivos no son suficientes, tenemos que exigir prevención y proactividad.

Por ejemplo, las firmas tradicionales siguen siendo imprescindibles para los antivirus en la actualidad, si bien debemos de adquirir soluciones que complementen esa capa de detección con buena tecnología heurística o basada en el comportamiento, capaces de detectar malware nuevo y desconocido.

No existe antivirus infalible, pero a buen seguro conseguiremos un mayor grado de protección.

En el caso del phishing debemos exigir a nuestras entidades sistemas de autenticación más robustos, utilizar el típico usuario y contraseña o PIN estático para el acceso y autorización de transacciones es a todas luces insuficiente.

Aunque son muchos los factores en contra a los que se debe enfrentar una entidad para implantar un sistema de autenticación multifactor y/o multicanal, la mayoría ajenos a la tecnología, la experiencia demuestra que cualquier avance, por pequeño que sea, es significativo en la lucha contra el phishing.

Un ejemplo, las tarjetas de coordenadas no dejan de ser un pseudo intento de OTP (One-Time Password) primitivo. A algunos le resultará contradictorio que en pleno siglo XXI tengamos que mirar una tarjeta de plástico y jugar a los barquitos para introducir una contraseña. Pero las entidades que las han implantado han visto reducir drásticamente su nivel de fraude por Internet.

Tampoco es, ni mucho menos, la solución definitiva. Sistemas más robustos que las tarjetas de coordenadas (certificados, tokens, canales alternativos vía móviles, etc.) pueden ser, y serán atacados, con efectividad. De hecho algunos de ellos ya son objetivos puntuales en la actualidad. Pero mientras existan entidades con sistemas más débiles, basados en el usuario y contraseña tradicional, los atacantes y el phishing se cebarán en ellos.

Resumiendo

Es una frase manida, pero no por ello le quita razón: la seguridad es un proceso continuo. No vamos a encontrar la solución mágica contra los ataques y el fraude, desconfié de quién le ofrezca el producto definitivo y 100% seguro.

Tampoco es menos cierto que la seguridad es una responsabilidad compartida. Aunque cada vez se tiende a hacer los sistemas de seguridad más transparentes para el usuario, pocos pueden resistir cuando no se hace un uso responsable de la tecnología.

Debemos de aprender a evolucionar en el tiempo. Como usuarios tendremos que informarnos continuamente sobre las nuevas amenazas que van surgiendo, no en vano la educación en materia de seguridad es una las principales y más útiles barreras contra los ataques. Nos tocará también adquirir nuevos hábitos y adaptarnos a nuevas tecnologías.

Pero, sobre todo, debemos exigir a los proveedores unos niveles mínimos de seguridad en todos los sistemas que nos rodean, desde la solución antivirus de nuestro PC pasando por la banca electrónica de nuestra entidad. A día de hoy muchos están por debajo de lo que exige la situación actual.

Tú eres el usuario, tú mandas, ¿hora de cambiar?.

Bernardo Quintero

18/12/2006 De compras en el supermercado del malware

eWeek publica una entrevista con Raimund Genes, director de sistemas de Trend Micro, en el que desvela los distintos precios que se pueden llegar a pagar por exploits para vulnerabilidades que todavía no han salido a la luz. Como quien va a al supermercado, existen de todos los tipos, gustos y precios.

Según parece, Trend Micro logró infiltrase en un especie de subasta donde se comercializaba con vulnerabilidades y exploits. Desde ahí ha logrado tomarle el pulso a los baremos económicos en los que se mueven las mafias informáticas hoy en día.

Por ejemplo, un exploit para una vulnerabilidad no pública que permite ejecutar código en Windows Vista ronda (según siempre declaraciones de Genes para eWeek) los 50.000 dólares (38.100 euros aproximadamente). Para otros sistemas, dependiendo obviamente de su popularidad y de la gravedad de las vulnerabilidades, los precios rondan los 20.000 a 30.000 dólares, entre 15.000 y 20.000 euros más o menos.

Uno de los tipos de troyanos más habituales hoy día, los que secuestran máquinas Windows que generan todo ese spam que inunda los buzones (indicador de la eficacia de estos ataques) se venden por unos 5.000 dólares (3.800 euros). Un troyano “a la carta” capaz de robar información sensible de cuentas online puede ser comprado por 1.000 ó 5.000 dólares. Un troyano que permita construir todo un botnet se puede comprar por 5.000 ó 20.000 dólares.

Si la idea de infectar y esperar beneficios no resulta atractiva, se pueden obtener directamente números de tarjetas de crédito con su correspondiente PIN por sólo 500 dólares (380 euros). Otros datos personales se venden por entre 80 y 300 dólares (de 60 a 230 euros).

Y no sólo malware y datos, según Genes, en la subasta también se vendían licencias de conducir falsas, certificados de nacimiento, números de seguridad social... Lo más "asequible" son las cuentas de eBay o PayPal, a 7 dólares cada una (5 euros).

Si estos son los precios que se pagan, los beneficios deben ser potencialmente mayores si se sabe gestionar el producto, no hay duda. El conocer cómo aprovechar una vulnerabilidad o un troyano "a la carta" y por tanto no detectable por la mayoría de antivirus (a no ser que posean unas excelentes heurísticas) supone un ingreso potencial de dinero que bien merece una inversión.
Esto demuestra una vez más que los creadores de malware poseen una motivación real para la producción de este tipo de código. Que es un "producto" que atiende a un mercado concreto y por tanto se rige por la ley de oferta y demanda que ha derivado en la situación actual: los niveles de infección por troyanos bancarios son altísimos, han desaparecido las infecciones masivas por un único virus, se explotan nuevas vías de infección (MS Office, principalmente) con numerosos "0 days" descubiertos, VirusTotal recibe decenas de nuevos troyanos bancarios al día (la mayoría no detectados)... todo buscando el máximo beneficio y rendimiento, entendiendo como tal un lucro real, tangible, económico.

Lejos están los románticos tiempos de gusanos masivos y virus molestos (pero inocuos a la postre). Estamos hablando de inversión y beneficios, con el auge de la banca online ha surgido una nueva posibilidad de negocio, un nuevo nicho de mercado que no ha tardado en ser ocupado y que, tal es la cantidad de dinero que mueve, que según Genes, éste superaría ya al volumen que maneja el mercado de las soluciones antimalware.

Sergio de los Santos



Desmantelando...









Capítulo 9

AÑO 2007

7D7

3727

11111010111



1215907200 – 1247443199



Durante este año...

_ Una entrada en el laboratorio de Hispasec, titulada **“Google, ¿el otro gran hermano?”**, escrita por Bernardo, reflexiona sobre los poderes que está tomando esta compañía en la recopilación de datos personales entre sus distintos servicios de Adsense, búsqueda, Gmail... Poco tiempo después (en cuanto, precisamente es indexado por Google) la entrada se convierte en un vertedero de comentarios (más de 200) de personas que quieren participar en el concurso televisivo Gran Hermano, tanto su versión argentina como española. Algunos agudos comentarios a la entrada son (literalmente):

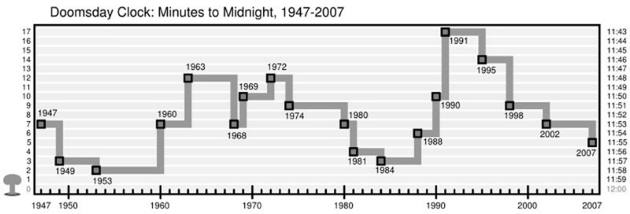
> *quisiera participar en gran hermano 5 porque me coincidero una adolescente fogosa que puede calentar la pantalla de telefe quisiera que me avisaran cuando y donde es el casting para gran hermano 5*
>
> *Posted by: paola pellicciotti at abril 24,2007 16:44*
>
> *quisiera saber si va a ver otro gran hermano por que me gustaria hace el casting para entrar a la casa soy de camapana bs as tengo 20años y seria una gran experiencia experiencia y aparte tengo cualidades para entrar en la casa y seria un gran paso para dedicarme a lo que me gusta que es la actuacion por favor envienmen las fechas y lugares donde se va a hacer el proximo casting desde ya muchas gracias*
>
> *Posted by: agustin lencina at abril 26,2007 03:3*
>
> *KIERO PERTICIPAR Y TARTAR DE JUGAR ESTE JUEGO LLENO DE HEMOSIONES ENCONTRADAS KIERO VIVIR ESA ADRENALINA DE ESTAR ENCERRADA POR MESES CON GENTE NUEVA PARA CONOCER Y TRATAR DE CONOCERME MAS A MI MISMA BUENO GRACIAS Y ESPERO ME NOTIFIKEN LAS ULTIMAS NOVEDADES*
>
> *Posted by: KISCHNER CAROLINA at abril 28,2007 04:08*
>
> *hola soy mary tengo 15 años casi cuplo los 16 pero me gustaria saver un poco mas de este proyecto porque me he sentido un poco sola desde hace un tiempo me gustaria que esto sea un ejemplo en mi vida y me gustaria participar no tengo tanta inspiracion para escribir pero hablo un montonazo. un besote bay*
>
> *Posted by: mary martinez*
>
> *“ HOLA GRAN HERMANO: me siento raro escribiendo esto, pero QUIERO ENTRAR A LA LOCURA DE ESA CASA...me llamo CRISTIAN tengo 25 por favor manden info para saber donde son los casting...*
> *BASTA DE MIRAR POR LA TELE Y DECIR YO TENGO QUE ESTAR AHI...AHORA LLEGO EL MOMENTO, ACA ESTOY TENGO UNA HISTORIA QUE CONTAR Y ESTOY LISTO PARA TODO LO QUE SE VENGA DESPUES...*
> *GRACIAS Y ESTOY LISTOOOOOOOO*
>
> *Posted by: cristian at junio 15,2007 18:29 ”*

_ Rumanía y Bulgaria pasan a formar parte de la **Unión Europea**. Cuenta ya con 27 países miembros.

_ Un petrolero sufre un accidente en aguas noruegas, vertiendo **200 toneladas de crudo** en el océano.

_ El 17 de enero se adelanta dos minutos el **reloj del apocalipsis** (Doomsday clock). Se trata del símbolo más representativo de peligro nuclear. Consiste en una esfera con el mapamundi grabado y dos agujas que no corren. Una, la de las horas, está permanentemente fijada en las doce. La otra, la de los minutos, ha sido movida en 19 ocasiones durante el último medio siglo. Se conserva desde 1947 en un edificio del campus

universitario de Chicago, sede de “The Bulletin of Atomic Scientist”. También es conocido como “El Reloj del Juicio Final”. Sólo ha variado 19 veces desde que se estableció. Se supone que la medianoche significará el fin de la Humanidad. Se rige por los dictados de la política mundial. Se estuvo a 17 minutos en 1991 tras la firma de los tratados de reducción de armamento entre la Unión Soviética y EE. UU. En 1953 tras las pruebas nucleares llevadas a cabo por las mismas potencias, se estuvo a 2 minutos del fín.



_ El 10 de febrero la **Wikipedia en español** alcanza los 200.000 artículos.

_ Durante la segunda mitad de enero se sufren **fuertes lluvias en toda Europa**. En el Reino Unido mueren 17 personas. En Alemania, son 13 las personas que se traga el agua. El huracán Kyrill arrasa el Oeste de Europa, dejando un total de 44 muertos en 20 países. Las tormentas serían la excusa para la primera oleada del “Storm worm”, que enviaba un spam con un adjunto prometiendo fotos de los sucesos.

_ El 20 de enero Microsoft lanza **Windows Vista** y Office 2007 finalmente al público. Principalmente por la carencia o los problemas con los drivers, el producto rápidamente se gana fama de inestable. También de devorador de recursos a causa de ciertas características que, en realidad, acaparan memoria para acelerar el lanzamiento de las aplicaciones. Por último, la estabilidad y comodidad que sienten los usuarios de XP, un sistema que fue publicado en 2001, y que en parte gracias al retraso de Vista se consolida fuertemente durante los años, hacen que el sistema operativo sea calificado de fracaso. Sin embargo, con respecto a la seguridad, supone una importante apuesta y mejora por parte de Microsoft. Es el primer sistema operativo desarrollado completamente dentro de su programa integral de seguridad.

Sony saca a la venta su nueva consola, PlaStation 3, en Europa. Es la primera consola con lector de Blu-Ray. Cuesta 600 euros en España (bastante menos después) y sus ventas son muy discretas esa Navidad, en parte por el precio, en parte por la novedad con la que



ese mismo año compite **Nintendo, la Wii**. Su lanzamiento es casi paralelo. Es la primera consola que contiene un mando que permite detectar el movimiento y la rotación en tres dimensiones. Sony ya había intentado huir de los mandos tradicionales desde su EyeToy hacía años. Se trataba de un periférico creado para la PlayStation 2. Básicamente una cámara que permitía que el jugador interactúese con lo que aparecía en la pantalla. No gozó de mucho éxito. Sin embargo, la Wii sorprendería a muchos por su precisión y novedad. El mercado se abría a jugadores de todas las edades que podían desde disparar hasta hacer ejercicio con la consola.

_ Hispasec lanza el 20 de febrero su primera herramienta gratuita para móviles en forma de aplicación Java (J2ME), **CryptaMobile**. Se trata de un pequeño programa de almacenamiento seguro de contraseñas.

_ En mayo desaparece **Madeleine McCann**. La niña de tres años está de vacaciones con sus padres y hermanos en un hotel de Praia da Luz, en el Algarve de Portugal cuando desaparece. El caso salta a los

medios y los padres convierten el asunto en un verdadero acontecimiento mediático con anuncios, logotipo de la campaña de búsqueda (basado en una mancha en el iris de Madeleine, una curiosa característica), recibimiento ante el Papa, recolecta de millones de dólares y apariciones en televisión. El mundo se vuelca y se identifica con ellos. Poco después los acontecimientos toman un giro inesperado cuando los propios padres se convierten en sospechosos. No se tienen pistas fiables de secuestro y se encuentra sangre en el coche que alquilan. Deben declarar. El caso se enturbia con ciertas diferencias entre la policía portuguesa e inglesa, que salen a la luz. Los padres continúan con la búsqueda ahora con fondos privados pero desde los medios son desde entonces rechazados y mirados con recelo.

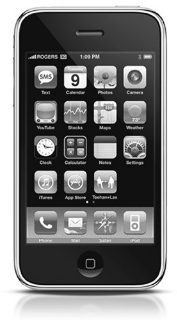
_ **Hispasec** dispone ahora de una página en inglés, www.hispasec.com/en/ sin una-al-día.

_ Se detectan una serie de ataques de denegación de servicio, coordinados e insistentes contra la infraestructura de Internet de **Estonia**. Muchas páginas oficiales de ministerios, servidores de correo institucionales y otras organizaciones dejan de estar operativas. El ataque resulta tan salvaje que el gobierno de ese país pide ayuda a la Unión Europea. Se especula mucho sobre quién puede estar detrás de estos ataques. En principio se culpa a Rusia, debido a tensiones diplomáticas entre ambos países, pero resulta imposible determinar de dónde proviene exactamente el ataque. Lógicamente se trata de redes distribuidas de sistemas zombi, repartidas por todo el mundo. El "hacktivismo" se pone de moda.

_ El 11 de marzo se publica una entrada en el blog titulada **"Sitio donde echar tu curriculum"**. En ella Bernardo cede un email para quien quiera enviar su currículum. La persona detrás de ese correo le ofreció trabajo como director de seguridad y obviamente lo rechazó. La entrada es indexada por Google y en poco tiempo, los comentarios se inundan con peticiones de empleo de lo más extrañas, desde profesores de educación física hasta personas que buscan trabajo "de cualquier tipo".

> *Re: Sitio donde echar tu curriculum*
>
> *hola busco trabajo en gijon tengo 16 años en octubre cumplo 17 soi muy trabajador 655XXXXXX llamarme*
>
> *Posted by: ivan at mayo 26,2008 16:51*
>
> *Re: Sitio donde echar tu curriculum*
>
> *holaaaa todos.......busco trabajo en lo q sea, pero me gusta mucho ser dependienta en tiendas de ropa.tengo 17 años y soy muy buena trabajadora y simpática.....lo necesito, y soy una chica que me encanta atender al público.si quereís yamarme al 6273XXXXXX ó 953XXXXXX.......gracias y esrtaré encantada de hacer una entrevista con ustedes y si es posible poder trabajar.....gracias y un buen abrazo chao*
>
> *Posted by: rocio at junio 25,2008 16:09*

_ Las bajas estadounidenses alcanzan los **3.500 militares muertos** desde la invasión de Iraq en marzo de 2003.



_ Se lanza en Estados Unidos el **iPhone**. Se trata del teléfono móvil multimedia más goloso hasta la fecha, creado por Apple, especialista en caprichos. También es el primer móvil totalmente táctil, sin posibilidad oficial de uso de puntero. La primera generación, que no llega a España, es cuatribanda GSM. A nuestro país llegaría a mediados de 2008 con el firmware 2.0 y conocido como iPhone 3G. El anuncio fue precedido por rumores y especulaciones que circularon durante varios meses. Esto no hizo más que crear expectación. Fue llamado por la revista "Time" el invento del año 2007.

_ En julio el senado de los Estados Unidos duplica a 50 millones de dólares la recompensa para quien capture vivo o muerto a **Osama Bin Laden**. Sigue en libertad y amenazando esporádicamente al mundo

occidental siete años después de los atentados de las Torres Gemelas.

_ En agosto se lanza **Google Earth Sky**, una evolución de Google Earth centrada en el espacio. En octubre de 2004 Google compró Keyhole, un programa de pago que Google ofrecería de forma gratuita y llamaría Google Earth a mediados de 2005. Poco a poco aumentaría sus servicios basados en la vista en satélite de la tierra y lanzaría Google Maps, con la posibilidad de calcular recorridos y muchas otras funcionalidades.

_ El 15 de agosto **Perú sufre un terrible terremoto** que mata a más de 500 personas y deja 1.500 heridos. Se lanza la alerta de un posible tsunami en el océano Pacífico.

_ En octubre se lanza **Ubuntu 7.10**.

_ El 16 de abril se produce la **masacre de Virginia Tech**. En el Instituto Politécnico y Universidad Estatal de Virginia (conocido como Virginia Tech), en Blacksburg, Virginia (Estados Unidos). Mueren 33 personas, incluyendo a Cho Seung-hui de 23 años, autor de la matanza. Se trata de un estudiante surcoreano que el mismo día de la masacre envía a la cadena NBC unos vídeos donde aparece disparando en modo amenanzante. Los vídeos se distribuyen rápidamente por YouTube, creando cierta polémica. El 7 de noviembre un estudiante mata a nueve personas en un instituto finlandés tras anunciar el crimen en Internet. El día antes el autor de los disparos había revelado sus planes en YouTube. El vídeo se titula **"Matanza en el instituto Jokela"**. Muestra una fotografía del instituto que se rompe. Luego aparecen dos imágenes en rojo de un joven que apunta a la cámara con una pistola. La historia se repetiría en Finlandia en septiembre de 2008. **Matti Saari** de 22 años cuelga en YouTube unos vídeos en los que aparece disparando a cámara mientras dice en inglés "Vosotros seréis los próximos en morir". La policía lo interroga un día antes de la masacre y decide que no es necesaria ninguna acción, aunque efectivamente posee una pistola Walther P22 como aparece en el vídeo colgado en la red. Matti Saari acude al Universidad de Ciencias Aplicadas de Kauhajoki en Seinäjoki e irrumpe a tiros matando a 10 compañeros y suicidándose luego.

Seguridad Informática



_ **Oracle anuncia por primera vez con antelación** sus publicaciones trimestrales de parches de seguridad. Un resumen previo al estilo Microsoft que adelanta el número y la gravedad de las actualizaciones previstas.

_ Comienzan a enviarse las primeras versiones de lo que se conocería como el **"Storm Worm"**. En una evolución sospechosamente parecida a la de Bagle en 2004, el virus comienza a inundar los buzones con spam que hace referencia a las tormentas que sufre en ese momento el norte de Europa. Durante todo el año, y aún hoy día, comienza una evolución imparable en la que pasa de ser un malware al uso a todo un sistema que, cada cierto tiempo, resurge modificado y en una nueva campaña temática de spam. Una de sus características más importantes es su capacidad de ofrecer componentes de descarga que mutan con una rapidez asombrosa. Prácticamente cada vez que se actualizaba la descarga, se tenía un troyano con distinto hash pero parecida funcionalidad. Es uno de los sistemas de malware más complejos y profesionales que se recuerdan.

_ A finales de enero se detecta un **phishing basado en la Agencia Tributaria (Hacienda)**. No ataca directamente a un banco (como viene siendo más que habitual). Lo que pretende es que la víctima

introduzca los datos de su tarjeta de crédito para que Hacienda le devuelva cierta cantidad. Posteriormente se detectarían todo tipo de phishings orientados a entidades y servicios que no son necesariamente bancos, incluso destinados a robar contraseñas de portales gratuitos.

_ El mes de enero, al amparo de la moda de los meses temáticos dedicados a las vulnerabilidades, se celebra **"El mes de los fallos en Apple"** por parte de LHM (que ya celebró el mes de los fallos en el kernel) y Kevin Finisterre. Publican un fallo del sistema Mac OS X o programas integrados en él cada día durante ese mes. Los errores encontrados salpican incluso a múltiples fabricantes, como el problema de PDF o el reproductor VLC Media Player.

_ En unas honestas declaraciones, **Natalya Kaspersky**, consejera delegada de la compañía especializada en sistemas antivirus, reconoce que necesita de la ayuda de las fuerzas del orden internacionales para proteger a los usuarios. Según ellos, los tiempos en los que se podía controlar la situación con los antivirus pertenecen al pasado.

_ El día 12 de febrero se da a conocer una **vulnerabilidad en Sun Solaris 10** tan simple como sorprendente. El fallo permite el acceso trivial como cualquier usuario (incluido root) a través de telnet en Sun Solaris 10. Sin necesidad de conocimientos especiales, sin shellcode ni exploits, el fallo llega a ser vergonzosamente simple. Para colmo, el error fue ya descubierto y corregido en sistemas UNIX hacía 13 años.

Michal Zalewski se da a conocer durante 2006 por su trabajo a la hora de poner a prueba la seguridad de los distintos navegadores. Descubre varias vulnerabilidades tanto en Internet Explorer como Firefox, dedicándose con especial hincapié a desafiar a este último navegador, al que sabe buscarle las cosquillas. Entre otros fallos, los torpedos de Zalewski (una serie de exploits que provocaban que el navegador dejase de responder) tumban el código de Firefox en varias ocasiones incluso después de aplicar actualizaciones. En febrero Zalewski vuelve a anunciar varios errores de diseño que considera constituyen serios problemas de seguridad. Zalewski es fiel seguidor de la filosofía de la revelación total de los detalles de las vulnerabilidades, lo que obliga a la organización Mozilla a retrasar la publicación de la última actualización para solucionar en ella algunos fallos descubiertos poco antes. La vulnerabilidad por la que Zalewski llega a calificar a Firefox como "el mejor amigo de los phishers", no es corregida y se publica Mozilla Firefox 2.0.0.2 con, además, otros fallos conocidos y explotables. Por si fuera poco, en una alerta oficial descolgada del resto, se anuncia que la última versión 2.0.0.2 del navegador Firefox también corrige una vulnerabilidad introducida por un parche anterior. El parche, publicado en diciembre, no sólo no corregía el fallo que pretendía sino que empeoraba la situación permitiendo la ejecución de código arbitrario.

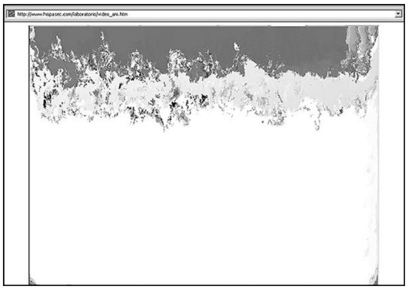


_ Microsoft anuncia que en marzo **no se publican boletines de seguridad**, circunstancia que no se daba desde septiembre de 2005. No significa que no existiesen fallos conocidos.

_ En marzo, los servidores oficiales desde donde se descarga el popular **WordPress** son comprometidos en algún momento y el código fuente del programa es modificado para troyanizarlo. Toda descarga producida desde el servidor oficial de WordPress desde el día 25 de febrero hasta el 2 de marzo de 2007 es susceptible de contener el código que permite acceso al servidor donde esté instalado.

_ Stefan Esser dedica marzo al **"mes de los fallos en PHP"**. Publica casi 40 vulnerabilidades en 31 días. Afortunadamente, la mayoría son problemas que no pueden ser aprovechados de forma remota. Stefan Esser es el creador de PHP, fundador de Hardened-PHP e impulsor del PHP Security Response Team. Durante años contribuye activamente al desarrollo de PHP y considera que el núcleo de programadores de este lenguaje no está concienciado con respecto a la seguridad. Por ello decide crear el mes de los fallos en PHP, como una especie de desafío hacia los programadores.

McAfee da a conocer el 28 de marzo una **grave vulnerabilidad en Microsoft Windows** que permite a atacantes ejecutar código de forma totalmente silenciosa a través de web. Se trata de un fallo en el tratamiento de archivos ANI que afecta a casi todas las versiones recientes de Windows. Poco después se hace público un exploit y los acontecimientos se precipitan. Los ataques se incrementan durante el fin de semana. Se publican hasta tres parches no oficiales (por parte de ZERT, eEye y X-Solve) y el oficial de Microsoft se adelanta para salir el día 3 de abril, rompiendo su ciclo habitual de los segundos martes de cada mes. El problema se basa en una vulnerabilidad ya conocida y solventada (al parecer no del todo), clasificada con el boletín MS05-002 por Microsoft y descubierta inicialmente por eEye. Los usuarios de Internet Explorer 7 en Windows Vista no se ven afectados debido al modo protegido de IE7. Tampoco prosperarían ataques a través de Microsoft Outlook 2007.



Hispasec publica poco después un extenso análisis técnico de la vulnerabilidad en ficheros ANI de Microsoft. Además, se publica una prueba de concepto en la que el visitante puede conocer la gravedad del problema. Con sólo visitar una web especialmente dedicada, se descarga y ejecuta desde Hispasec un pequeño programa que "derrite" la pantalla.

_ En abril Sophos publica un informe con interesantes conclusiones sobre la evolución del malware en los últimos tiempos. Se extrae que el **número de nuevas amenazas se han multiplicado por dos** en el último año, y que la web se vuelve el primer vector de ataque para intentar infectar a las víctimas. Desde VirusTotal y de forma independiente, llegábamos a conclusiones muy parecidas.

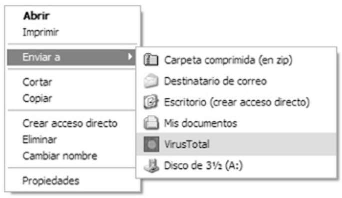
_ Se detecta una **nueva tendencia del malware** que mezcla phishing y troyanos. El atacante lanza un troyano que haga capturas genéricas o concretas de entidades bancarias. En los equipos que logra infectar, el troyano va enviando al servidor las URLs y datos de los formularios seguros por los que navega el usuario. El atacante va examinando los datos que le van llegando al servidor, buscando entre las URLs capturadas webs de banca electrónica, y prepara páginas de phishing específicas en base a las entidades que más se repiten entre los usuarios infectados. Es la corriente rusa. Desde el servidor indica a los troyanos que cuando el usuario navegue por ciertas páginas de banca los redirija a los contenidos de los phishings que ha preparado. A partir de entonces, cuando los usuarios infectados quieren visitar la página de su banco, el troyano los redirige a la falsa.

_ A rebufo de los periodos temáticos de vulnerabilidades, se anuncia en varias listas que el día 2 de abril comenzaría **la semana de los fallos en Windows Vista**. Incluso se publica una supuesta primera vulnerabilidad. Días después los autores destapan el engaño y confiesan que todo se trata de una broma, urdida alrededor del "día de los inocentes" anglosajón y perfectamente orquestada con alevosía y premeditación. Aprovechando el tirón mediático de los periodos temáticos, tomaron a Vista como objetivo,

para hacer la broma más atractiva hacia quienes consideraban su objetivo principal: Los medios. Con sólo anunciar su idea en Bugtraq consiguieron posicionar la página bien alto en Google. Páginas especializadas y genéricas pican y tragan el anzuelo, a pesar de que la vulnerabilidad publicada carecía de base técnica e incluso incluía guiños en su descripción que dejaban claro que el problema era inventado.

_ Se encuentra una vulnerabilidad en el sistema **DNS de Microsoft Windows** que puede ser aprovechada por atacantes remotos para ejecutar código en el sistema. El problema se debe a un desbordamiento de memoria intermedia en la implementación de la interfaz RPC del servidor DNS (Domain Name System) de Windows a la hora de procesar peticiones mal formadas enviadas a un puerto entre el 1024 y 5000. Se crean varios exploits que permiten aprovechar el fallo. En especial, uno programado por Andrés Tarascó y Mario Ballano es capaz de aprovechar la vulnerabilidad sin necesidad de tener acceso al rango de puertos mencionados en un principio (1024-5000), sino que permite ejecutar código a través del puerto 445.

_ Hispasec participa junto (pero no revueltos) con Microsoft en **una gira de seguridad** liderada por Chema Alonso que consiste en una serie de charlas, conferencias y mesas redondas en distintas ciudades de España. Durante abril y hasta junio se visitan, entre otras, Valladolid: Bilbao, Zaragoza, Pamplona, Valencia, Murcia, León... Además de Madrid y Barcelona en sus respectivos "Security Days".



Se pone a disposición de todos **VirusTotal Uploader**. Una pequeña utilidad para enviar muestras a VirusTotal. Una vez instalada se añade la opción "Enviar a -> VirusTotal" en el menú contextual de Windows. Cuando se envía el archivo se obtiene la respuesta del análisis a través de la interfaz web. Un año después, es seleccionada por la edición USA de PC World para pertenecer a su lista de **"101 Fantastic Freebies"**. Se trata de una prestigiosa lista anual de 101 utilidades software gratuitas (normalmente para Windows) que PC World recomienda especialmente. La votación es llevaba a cabo por lectores y personal de la propia revista.

Las categorías contempladas son:

Productivity (productividad), File Sharing and Storage (almacenamiento y compartición de ficheros), Security (seguridad), System Backup and Utilities (respaldo de sistema y utilidades), Maps and Directions (mapas y direcciones), Communications (comunicaciones), Time Management (manejo de tiempo), Music (música), Desktop Customization (personalización del escritorio), News Readers (lectores de noticias), Games (juegos).

En el apartado de seguridad, "VirusTotal Uploader" encabeza la lista, junto con programas tan reconocidos como Avira AntiVir PersonalEdition, Spyware Doctor Starter Edition, Comodo Firewall Pro, TrueCrypt, Secunia Personal Software Inspector, Spamfighter Pro, BitDefender Online Scanner, ThreatFire Free y McAfee Rootkit Detective.

En mayo de 2007 la edición americana de PC World premia a VisusTotal, dentro de los premios a los 100 Mejores Productos del Año 2007. Se reconoce a VirusTotal como el mejor sistio web de seguridad.

_ En mayo, **Rock Phish**, grupo pionero en ataques phishing en el mundo y responsable de la mayoría de ellos, dispara el número de ataques eludiendo leyes y contramedidas técnicas. Según algunas fuentes Rock Phish no es más que un kit de desarrollo de phishing rápido para inexpertos. Sin embargo Rock Phish es también una de las bandas más peligrosas y efectivas a la hora de crear ataques fraudulentos de robo de credenciales. Por ejemplo, tienen la capacidad de crear múltiples y únicas URL para cada ataque, muy complejas (es una de sus señas de identidad) que limitan de forma muy eficaz la labor de las barras antiphishing basadas en listas negras. Además, actúan a lo grande, pues son responsables de aproximadamente, más de la mitad de todo el phishing creado en el mundo en esos momentos.

_ En mayo se detecta **Badbunny**, una prueba de concepto que aprovecha las macros de OpenOffice. Se trata de malware sin repercusión. Trata de descargar una imagen JPG que representa a un señor vestido de conejo realizando un acto sexual. Lo curioso de este malware es que se distribuye a través de un documento OpenOffice Draw (badbunny.ODG) que, según el sistema operativo donde se ejecute, intenta infectar de diferentes formas.

_ **Robert Alan Soloway**, un importante spammer de 27 años responsable de una buena parte del correo basura mundial, es sentenciado por un juzgado de Seattle y se enfrenta a una pena de hasta 65 años de cárcel por fraude, robo de credenciales y blanqueo de dinero. Aunque se supone una buena noticia, ni experiencias previas ni el estado actual de la industria del malware hacen pensar que la situación para los que sufren el spam vaya a cambiar demasiado, como efectivamente ocurriría. El spam es cada vez más responsabilidad de las redes de zombis y menos de spammers profesionales. El spam es todavía uno de los pilares de la industria del malware. Como en la naturaleza, en cuanto un nicho queda vacío, alguien al acecho no tarda en ocuparlo. Ley de la jungla en Internet.

En junio siguen las campañas de envío del **"Storm worm"**, más virulentas si cabe. Prácticamente ningún antivirus, a estas alturas, se pone de acuerdo ya con los nombres de las variantes. Ocurriría ya habitualmente con todo el malware: clasificarlo de forma efectiva bajo un nombre concreto es imposible. Se recurre a los nombres genéricos de familias completas y aun así es complicado encontrar nombres iguales en las distintas casas. Hace tiempo que no se recuerda una epidemia tan duradera. Si bien no se percibe igual que en los tiempos del Klez, Code Red, Nimda o MyDoom, los niveles de infección pueden ser parecidos. Y no se percibe igual porque ya no es sólo que el Storm Worm mute con nuevas versiones, sino que se convierte en un complejo sistema multi-modular que se sirve de cientos de servidores comprometidos o no, una capacidad de mutación endiablada, y una modularidad que permite que sus funcionalidades cambien continua y radicalmente. Storm Worm ya no se podría clasificar como un troyano sino como un complejo sistema perfectamente orquestado, cambiante y eficaz. Muy al estilo malware 2.0. En septiembre, Microsoft incluye la firma de un componente de Nuwar (como lo ha bautizado) en su "Malicious Software Removal Tool". En 15 días elimina el troyano de 274.000 máquinas.

_ La compañía antivirus Sunbelt da la voz de alarma a finales de marzo. Se utiliza contra ella un tipo de ataque personalizado que **rompe las reglas habituales del spam masivo, impersonal y poco sofisticado**. Una supuesta carta de la BBB (Better Business Bureau), perfectamente personalizada y redactada, insta a la ejecución de un programa. Al parecer este malware infecta a más de 1.400 directivos. En el correo se explica que alguien ha interpuesto una queja contra la compañía y se pide la descarga de una supuesta imagen que resulta en realidad un ejecutable. BBB es una organización americana que

arbitra entre usuarios y consumidores, una especie de oficina del consumidor. En el correo electrónico, con una cuidada ortografía, se menciona con nombres y apellidos a personas reales pertenecientes a la empresa (habitualmente directivos), de forma que la primera impresión es que la acusación interpuesta puede ser real y que verdaderamente alguien se ha quejado de los servicios de la compañía. En otras versiones todavía más sofisticadas de la estafa, se usa un documento RTF adjunto en el que se incrusta un objeto OLE que no es más que un archivo ejecutable.

_ El día 7 de junio, se descubre una grave vulnerabilidad en unos **ActiveX de Yahoo! Messenger** que permite la ejecución de código arbitrario a través de la web. El código necesario para aprovechar el problema se hace público, y obliga a Yahoo! a publicar, apenas unas horas después, una nueva versión de su producto. Hispasec ofrece una prueba de concepto para que cualquiera pueda comprobar a qué se está expuesto con esta vulnerabilidad. Posteriormente Yahoo! tomaría la precaución de activar los kill bits de muchos de sus ActiveX a través de actualizaciones oficiales de Microsoft.

_ **MySpace** se convierte en el mes de junio en el objetivo primordial de ataques phishing perpetrados por la banda bautizada como Rock Phish. Cientos de miles de páginas creadas cada día para engañar a los usuarios de esta red social.

_ Se populariza el **spam en formato PDF**, en un intento (exitoso, pero poco duradero) por evitar los filtros antispam. Este tipo de ficheros no están contemplados por las soluciones antispam y, durante algunas semanas, se tragan sin marcar como basura este tipo de archivos. Para dificultar su detección, incluso incluye imágenes borrosas dentro de los propios archivos PDF. Poco después llega una nueva variante muy similar pero que utiliza la extensión .FDF en los archivos adjuntos. El ataque remitiría cuando los filtros antispam se actualizaron. Pocos meses después volvería a intentar el envío de PDF pero esta vez sería para aprovechar una vulnerabilidad en el lector Acrobat Reader.



En julio **VirusTotal se presenta con nueva imagen**. Desde su estreno en junio de 2004, el portal no había sufrido cambios estéticos destacables. Si bien su sistema de funcionamiento ha evolucionado considerablemente desde sus comienzos, VirusTotal se renueva además con una imagen mucho más limpia, sencilla y moderna. Alcanza en solo tres años un puesto muy reconocido entre los profesionales de la seguridad. Son muchos los CERTs, laboratorios, portales y usuarios en general que hacen uso diario de VirusTotal para el análisis de muestras sospechosas. Se ha convertido en el estándar "de facto" como herramienta para comprobar el estado de detección del malware por parte de los diferentes motores antivirus. Curiosamente desde sus inicios, e independientemente del número de muestras, los porcentajes se han mantenido estables. El 70% de las muestras son detectadas como malware. Desde 2005 además, un 30% de esa cantidad es detectado como malware específico para robar contraseñas de banca electrónica.

_ **El verano es duro para los navegadores**. Durante estos días, se descubren varias vulnerabilidades en (casi) todos los navegadores, además de problemas en conectores (plugins) tan habituales en ellos como Java y Flash Player.

_ Un investigador anónimo dice haber programado un **gusano para Mac OS X**, el sistema operativo de Apple. El gusano aprovecharía una vulnerabilidad todavía no parcheada que él mismo ha descubierto. El código no se hace público, por lo que parece que Rape.osx (nombre con el que se ha bautizado el supuesto gusano) tiene más de mediático que de proeza técnica.

_ En julio se descubre un **fallo en la predicción de identificadores de transacción en BIND**. Podría ser aprovechado por un atacante para envenenar la caché DNS. Un atacante podría averiguar por análisis criptográfico aproximadamente un 10% de identificadores de consulta. Suficiente para realizar un ataque. El problema se basa en que los identificadores no son calculados con la suficiente aleatoriedad. Este eterno problema de los servidores DNS volvería con muchísima más fuerza en el verano de 2008.

_ **La rama 8.x de BIND**, uno de los servidores de nombres más populares, deja de ser mantenida por el ISC (Internet Systems Consortium). No se publican más parches de seguridad para esta versión. Sus esfuerzos de desarrollo, a partir de ahora, se centran en la rama 9.x.

_ Sourcefire (compañía de Martin Roesh, el creador de Snort) anuncia la **compra de ClamAV** a los cinco líderes del popular proyecto "open source". Como era de esperar, el anuncio suscita todo tipo de reacciones en la comunidad ClamAV. El antivirus se mantendría sin demasiados cambios.

_ La página web del **banco de la India** es atacada de alguna forma y se convierte en foco (involuntario) de infección para usuarios de Windows que no tengan su sistema actualizado. Visitando la página web legítima y real del banco, el usuario queda irónicamente infectado por varios troyanos bancarios destinados a robar sus contraseñas de acceso a la banca online. Esta tendencia se repetiría hasta la saciedad. Vulnerar la seguridad de sitios web conocidos e incrustar código que permite aprovechar algún fallo es una técnica que sería usada de ahí en adelante cada vez con mayor eficacia.

_ A finales de agosto, alguien apodado Egerstad desde Suecia, publica en su blog las **contraseñas de cien cuentas de correo pertenecientes a instituciones gubernamentales de todo el mundo**. Fueron, paradójicamente, obtenidas a través del popular TOR, una red para hacer anónimo el tráfico en Internet. El atacante creó un nodo TOR, algo a disposición de cualquiera, y lo ofreció a la comunidad. Gracias al uso de TOR, con el que sus "víctimas" se sentían seguras, Egerstad consiguió esta información confidencial que colgó en su web.

_ Hispasec está en el **"Roll of honour"** de los phishers. En el Antiphishing Working Grupo (APWG) se hace público uno de los scritps encontrados en una página de phishing. En una "lista negra" de hosts, tal que así:

```
$IP = getenv("REMOTE_ADDR");
$host = gethostbyaddr($IP);
$banhosts = array("scotiabank","netcraft.com", "ebay.com", "panda.com","microsoft.com", "fbi.gov", "google.com", "msn.com", "yahoo.com", "cia.gov", "$resuelveserver", "bankofamerica", "mozilla", "viabcp", "veritas", "nod32","antipishing","kapersky", "norton", "symantec", "rsasecurity", "bancopopular", "paypal", "unicaja", "movistar", "banesto", "cajamadrid", "bancopastor", "rsa.com", "symantecstore", "gfihispana", "fraudwatchinternational", "verisign", "markmonitor", "anti-phishing", "pandasoftware", "delitosinformaticos", "zonealarm", "alerta-antivirus", "vsantivirus", "nortonsecurityscan", "hauri-la", "cleandir", "trendmicro", "mcafee", "nod32-es", "pandaantivirus", "free-av", "grisoft", "bitdefender-es", "sophos", "activescan", "avast", "bitdefender", "trendmicro-europe", "clamav", "clamwin", "eset", "symantecstore", "f-secure", "hispasec", "vnunet", "seguridad", "security", "monitor", "detector");
```

aparece el nombre de Hispasec. La idea de los atacantes es que si se visita el sitio phishing desde una IP cuya resolución inversa contenga alguna de esas cadenas, en vez de visualizar la página fraudulenta, el servidor devuelve un error 404. En definitiva, un intento para bloquear el phishing y dificultar su detección temprana o que se tomen medidas de cierre.

_ **La FIA (Federación Internacional de Automovilismo)** publica en su web las transcripciones de las reuniones sobre el caso de espionaje Ferrari vs. McLaren. Antes de su publicación, el borrador del documento fue revisado por Ferrari y McLaren para que indicaran el contenido confidencial que los protagonistas revelaron en sus declaraciones, como por ejemplo datos sensibles o relativos a su tecnología, cuyo conocimiento precisamente desata la investigaciónn y posterior sanción. La FIA lo publica en su servidor web en formato PDF. La visualización del documento muestra algunas porciones del texto ocultas por un rectángulo negro superpuesto, pero el texto original continúa ahí debajo, al alcance de cualquiera, a golpe de ratón.

_ Se publica una potencial **vulnerabilidad en Adobe Acrobat Reader** que podría permitir a un atacante ejecutar código arbitrario. Su descubridor no da detalles sobre la vulnerabilidad, pero afirma que un atacante podría fabricar un archivo PDF especialmente manipulado y hacer que se ejecute código arbitrario en Windows si es abierto con Adobe Acrobat Reader. El autor es el mismo investigador (Petko D. Oetkov) que da a conocer días atrás la vulnerabilidad en QuickTime Player a través de Firefox. Sería aprovechada activamente por atacantes para descargar un ejecutable e infectar sistemas.

_ Microsoft decide, después de un año, hacer que la **versión 7 de su navegador** esté disponible libremente para todo el mundo, independientemente de que su Windows demuestre ser "genuino" y original.

_ En octubre se bate el **récord de archivos procesados por VirusTotal en 24 horas**. Se superan las 40.000 muestras procesadas por VirusTotal en 24 horas. 17 análisis por segundo. El récord volvería a ser roto poco después. En noviembre se establecen los **permalinks** para VirusTotal. Con ellos se puede almacenar para siempre un enlace con el resultado de una muestra enviada.

_ **El malware en forma de supuesto codec parece "consolidadarse" contra usuarios de Mac**. Sigue la "moda" de introducir malware en los sistemas usando como reclamo la necesidad de codecs específicos para poder reproducir un vídeo. Estos codecs suelen ser ejecutables para Windows, aunque también los sistemas Mac se ven afectados. Usan el user-agent del navegador para distinguir qué sistema operativo visita la web y descargar el malware correspondiente.

_ En Hispasec se detecta un **ataque phishing a gran escala contra entidades bancarias españolas** que además intenta troyanizar el sistema. El kit de phishing afecta a 35 organizaciones, todos en un mismo servidor.

_ En noviembre se realiza un envío masivo de un mensaje que invita a visualizar un supuesto vídeo en YouTube. El reclamo en esta ocasión es reproducir el célebre incidente entre el Rey de España y el Presidente de Venezuela. **¿Por qué no te callas?** Esta técnica se haría bastante popular con otros temas de moda.

_ Se encuentra una **vulnerabilidad en un software preinstalado en muchos portátiles HP**. Al tratarse de un ActiveX, el usuario de estos portátiles que utilice el software por defecto del fabricante y que visite con Internet Explorer alguna página especialmente manipulada, podría ejecutar código inadvertidamente.

_ Un informe de la empresa de investigación de mercado **Gatner** habla de unas pérdidas de **3.200 millones de dólares** por culpa del phishing en 2007. El informe pone cifras al phishing "tradicional", contabilizando desde agosto de 2006 a agosto de 2007 y centrado en Estados Unidos.

_ En Hispasec se detecta un nuevo método de fraude bancario que aprovechaba **vulnerabilidades de routers** para realizar un pharming. Consiguen modificar los DNS del ordenador a través de fallos en los parámetros del router. Se centran en Banamex.

Una al día

22/01/2007 El mediático troyano de la tormenta y las lecciones no aprendidas

"Storm Worm" o "Storm Virus" se ha popularizado en las últimas horas como malware de rápida distribución que ha llegado a miles de sistemas. Lo oportuno del asunto original con el que aparecía en los buzones (haciendo referencia a la tormenta que ha azotado Europa), ha provocado que muchos usuarios lo ejecuten y queden infectados. Resulta llamativa su capacidad de infección teniendo en cuenta que "Storm" es un malware con un método de infección "de manual", tradicional y sin ninguna capacidad técnica que llame la atención.

El viernes F-Secure alertaba de una rápida propagación de un troyano llamado por algunas casas Small. DAM (más conocido como "Storm"), que llegaba a través del correo electrónico. En la noticia publicada (acompañada de un mapa del mundo muy vistoso) se podían seguir a través de luces parpadeantes la velocidad de infección del malware en cuestión.

Técnicamente hablando Small.DAM no aporta nada nuevo, ni en su técnica de expansión ni en su daño potencial: Es una variante de Small, es un "downloader" para sistemas Windows, instala un nuevo servicio y tiene propiedades de puerta trasera con lo que el sistema quedaría a disposición de, probablemente, un operador de botnet. Nada que destacar hasta el momento.

La versión original detectada el viernes 19 de enero se propagaba a través del correo, en un archivo adjunto ejecutable para sistemas Microsoft (.exe) y con asuntos como:

* 230 dead as storm batters Europe (230 muertos en una tormenta que arrasa Europa)
* Saddam Hussein alive! (¡Saddam Hussein vivo!)

Y adjuntos con la carga maliciosa con nombres como:

* Full Clip.exe
* Full Story.exe
* Read More.exe
* Video.exe

Un ejemplo "de libro" sobre ingeniería social sencilla a la hora de intentar engañar a los usuarios. Este virus no ha necesitado aprovechar ningún tipo de vulnerabilidad, esconderse bajo extensiones aparentemente inofensivas, ni partir de una familia previamente no detectada de malware. Simplemente, ha usado una

noticia actual y suficientemente morbosa (la promesa de un vídeo sobre los que han sufrido mortalmente el temporal o la hipótesis de un dictador vivo cuando medio mundo ha presenciado su ejecución) para conseguir cierto éxito y propagarse sin dificultad. Una muestra más del eslabón más débil de cualquier cadena de seguridad: el usuario.

Ante el éxito, la pista se pierde. En las últimas horas han aparecido decenas de variantes, con nuevos asuntos, adjuntos y carga vírica. En sus últimos análisis, se observan inclusos comportamientos de rootkit para ocultarse en el sistema.

Las últimas actualizaciones de la mayoría de los antivirus están añadiendo a marchas forzadas firmas para detectar las muchas variantes producidas. Se recomienda en cualquier caso, aplicar el sentido común y no ejecutar archivos ejecutables no solicitados. Si los administradores todavía no lo han hecho, se deberían descartar los archivos ejecutables a nivel de pasarela de correo.

Sorprende (y decepciona) que acudir a técnicas de propagación tradicionales y carentes de imaginación como este malware (que confía sólo en el poder de un asunto llamativo para su propagación), resulte exitoso a estas alturas. Es una lección que, por repetición desde hace ya muchos años, creíamos aprendida.

Sergio de los Santos

06/02/2007 Kaspersky reconoce que no puede hacer milagros

En unas honestas declaraciones, Natalya Kaspersky, consejera delegada de la compañía especializada en sistemas antivirus, reconoce que necesita de la ayuda de las fuerzas del orden internacionales para proteger a los usuarios. Según ellos, los tiempos en los que se podía controlar la situación con los antivirus pertenecen al pasado.

ComputerWorld recoge unas sorprendentes declaraciones de una de las compañías antivirus más reconocidas mundialmente. En ellas piden la cooperación de la policía internacional: “No tenemos las soluciones. Pensamos que era posible realizar antivirus y eso ofreció una protección adecuada. Ya no es así”. “Solucionar el problema está más allá de las capacidades de los fabricantes de productos de seguridad en solitario. Se necesitan esfuerzos coordinados entre los países”.

Desde Kaspersky también reconocen que están abrumados. “La compañía tiene a 50 ingenieros analizando el nuevo malware y buscando formas de bloquearlo, pero con 200 nuevas muestras por día, y en aumento, el trabajo se hace arduo”. “Ninguna compañía antivirus puede venir y decirte que puede manejarlo todo. Consideramos responsable hacerlo saber a la gente de forma clara.”

El “Center for Strategic and International Studies” (que asesora a gobiernos en cuestión de seguridad), y una comisión federal de comercio se unirán a Kaspersky para hacer una llamada a las fuerzas del orden, para que se involucren más en la lucha contra los creadores y distribuidores de malware. Intentarán llega a acuerdos internacionales para crear las condiciones adecuadas que permitan perseguir a los criminales a través de las fronteras”.

Reconocen que el éxito de la policía en este sentido ha sido limitado, con apenas 100 detenciones por año. “Sólo los estúpidos se dejan coger. A los listos es muy complicado encontrarles”, afirma Kaspersky.

Por último, Kaspersky añade: “El software destinado a bloquear el malware es efectivo, pero no puede parar todos los ataques. Somos como la policía, nos perdemos muchos casos pero hacemos lo que podemos. Intentamos prevenir, pero no podemos hacer milagros”.

Kaspersky asume así la nueva situación vírica mundial de forma honesta y responsable.

Sergio de los Santos

13/02/2007 Phishing, el “hermano pobre” de los troyanos

El phishing sigue siendo la práctica fraudulenta por Internet más visible y reconocida, ya que el spam masivo de correos invitando a los usuarios a que visiten una página falsa puede ser detectado por cualquiera. Por contra, de los troyanos especializados en el robo de claves se saben que existen y están ahí, aunque no son tan reconocidos ni se ven a simple vista. ¿Qué técnica de estafa es más peligrosa? ¿Con cuál se están obteniendo mayores resultados y beneficios?

Primero hay que dejar por sentado que si tanto phishing como troyanos de robo de contraseñas siguen proliferando es, simplemente, porque con ambas técnicas los estafadores obtienen beneficios.

Las principales diferencias entre una técnica y otra, pensando en la rentabilidad de los estafadores, son:

* Exposición: cómo ya hemos comentado al inicio, un ataque phishing tradicional, no segmentado o dirigido, queda expuesto a cualquiera desde el lanzamiento del spam, incluso en muchas ocasiones se aborta antes de que sea público a través del spam.

El troyano no puede detectarse antes de que sea público (nos referimos a la detección del sitio donde envían los datos, no a la detección de la muestra en sí que sí puede ser detectada por un antivirus desde el minuto 0), y la distribución puede ser más silenciosa y pasar desapercibida al no ser tan evidente como un phishing.

* Esperanza de vida: por la exposición, un ataque phishing se detecta e intenta mitigar/cerrar desde el primer momento. Dependiendo de la insistencia del equipo de cierre y de la profesionalidad/colaboración de los responsables del sitio donde se hospede, el ataque puede estar “vivo” durante minutos, horas, o a lo sumo algunos días.

La esperanza media de vida de cada una de las variantes de un troyano suele ser de varias semanas o meses, dependiendo de cuando es detectado por un servicio antifraude y se cierra el destino a donde el troyano envía los datos.

* Alcance: en el phishing tradicional cada ataque va destinado a una entidad en concreto, ya que tanto el e-mail como la página están personalizadas para imitar a una determinada entidad.

Por otra parte, una sola variante de un troyano suele dirigirse a un mayor número de entidades, normalmente varias decenas, o directamente capturar datos de forma indiscriminada que después pueden ser fácilmente filtrados en el servidor que recibe los datos.

* Dificultad: un ataque de phishing tradicional es relativamente muy fácil y rápido de montar sin necesidad

de grandes conocimientos, lo que explicaría que aun no siendo tan productivo como un troyano siga siendo una práctica habitual.

Los troyanos conllevan una mayor dificultad en su diseño, requiere más conocimientos avanzados de programación que un phishing, sin embargo también se está popularizando la venta en foros underground de kits de troyanos "banker" que facilitarían los ataques a estafadores menos preparados.

* Calidad: en el phishing tradicional son muchos los usuarios que, a sabiendas de que se trata de un fraude, introducen en las páginas de phishing información falsa para confundir a los estafadores. Por nuestra experiencia, en la que hemos accedido a servidores de phishing, en los datos introducidos se encuentran desde contraseñas falsas hasta mensajes o insultos hacia los estafadores, el porcentaje de información útil y aprovechable es pequeña, aunque suficiente para que sea rentable (aunque los que "piquen" se puedan contar con los dedos de una mano).

Por el contrario, los datos capturados por los troyanos son en su inmensa mayoría auténticos, ya que el usuario no es consciente de que de forma oculta los datos introducidos en las páginas webs legítimas están siendo a su vez reenviados al servidor de los estafadores. Además el volumen de datos recolectados es muy superior al que puede lograr cualquier ataque phishing, de hecho los estafadores sólo explotan una parte de lo que capturan con este tipo de ataques (se centran en las entidades que les ofrecen "mayores ventajas" a la hora de hacer las transferencias y el blanqueo a través de las mulas).

Como ejemplo de lo que un troyano puede recolectar, se pueden encontrar datos de un caso real en la siguiente dirección del blog del Laboratorio de Hispasec:

"Un día en la vida de un troyano 'banker'":
http://blog.hispasec.com/laboratorio/195

Bernardo Quintero

21/06/2007 Resaca del ataque masivo a través de webs comprometidas

El pasado día 19 alertábamos de un ataque a gran escala contra webs europeas, que tenía como último objetivo robar las claves de acceso a la banca por Internet de los usuarios que las visitaran. Después del aviso el ataque fue neutralizado en menos de 24 horas, a día de hoy podemos ofrecer nuevos datos sobre el incidente.

Más de 11.000 páginas webs fueron modificadas para redirigir a sus visitantes de forma oculta a un tercer servidor web malicioso. El usuario afectado en ningún momento era consciente de nada anormal, veía con normalidad la web a la que se había dirigido, toda la conexión maliciosa se hacía en un segundo plano.

Si el usuario que visitaba alguna de esas 11.000 webs lo hacía con una versión vulnerable de Windows (si no había instalado algunos de los parches de seguridad distribuidos por Microsoft durante 2006), automáticamente se introducía en su ordenador un troyano que podía robarle las claves de acceso a su banco por Internet.

Resumen cronológico

La herramienta utilizada para realizar las infecciones a través de las webs comprometidas fue MPack

0.86. Esta herramienta ya fue motivo de un detallado análisis por parte de Panda Labs el pasado mes de mayo, y se viene utilizando asiduamente desde el año pasado en ataques similares. También en mayo el blog de Symantec Security Response dedicó una entrada a las funcionalidades de MPack.

Websense alertó el día 18 de este mes sobre un ataque masivo a 10.000 páginas webs basándose en la herramienta MPack 0.86. Hispasec también pudo acceder al servidor MPack utilizado por los atacantes y tener acceso a los datos del incidente ese mismo día. Tras un avance en el blog del Laboratorio de Hispasec la madrugada del 18, alertamos el día 19 a través del boletín una-al-día actualizando y aportando nuevos datos.

Al finalizar la jornada del día 19 se logró mitigar el ataque, al desactivar el servidor web malicioso al que se redirigían los más de 11.000 sitios webs comprometidos.

Los días 19 y 20 la noticia saltó de los círculos de seguridad a los medios de comunicación, y terminó acaparando espacio en prensa, radio y televisión. Lo que más llamó la atención fue el número de webs comprometidas, y el hecho de que los usuarios podían infectarse con tan sólo visitar una web “normal”. En medios internacionales el protagonismo se lo llevó la herramienta utilidad en el ataque, MPack.

Hispasec en su blog del Laboratorio apuntó a que las más de 11.000 webs comprometidas se hospedan en un mismo proveedor italiano, Aruba, y que por tanto el ataque tan voluminoso fue posible por un problema de seguridad en la infraestructura del proveedor de hosting. Hoy, día 21, SANS Internet Storm Center publica una nota de Verisign/Idefense que apoya la misma conclusión que Hispasec, y apuntan a que el ataque al proveedor de Internet pudo realizarse a través de una vulnerabilidad en la herramienta cPanel de administración web.

Mientras continúa la resaca informativa de este caso, a buen seguro se están sucediendo otros incidentes similares, incluyendo los que estén utilizando la nueva versión MPack 0.90. Entre las novedades de esta versión destaca el uso de la vulnerabilidad ANI, cuyo parche para Windows fue publicado por Microsoft en abril de 2007, y que dota de un mayor poder de infección a las nuevas webs comprometidas.

También se incluyen el uso de vulnerabilidades de aplicaciones de terceros muy difundidas en Windows, como WinZip y QuickTime, que por norma general los usuarios descuidan más su actualización.

MPack 0.90 también corrige algunos problemas de seguridad de la propia herramienta, que permitía que empresas como Hispasec pudieran acceder a los servidores de los atacantes y tener datos puntuales sobre lo que estaba sucediendo, motivo por el cual hemos podido informar con tanta precisión sobre el alcance de este ataque y ayudar en su mitigación. Estas nuevas mejoras entorpecerán conocer la envergadura real y exacta de los nuevos ataques que se sucedan, si bien la lucha se mantendrá viva entre los atacantes y las empresas de seguridad.

Moraleja

Aunque la mayoría de las informaciones se han centrado en MPack como herramienta de ataque, en Hispasec creemos que la lectura más útil del incidente va encaminada a concienciar a los usuarios finales.

Realizar una navegación responsable no evita la posibilidad de sufrir ataques. Hay cierta tendencia a pensar que los usuarios que se infectan es porque necesariamente han visitado páginas webs “peligrosas” (contenidos eróticos, descarga de programas piratas, cracks, etc). Es cierto que visitando esas páginas puede existir mayor probabilidad de infecciones, especialmente con la instalación de cracks dependiendo

de la fuente, pero también sucede en otras páginas webs con contenidos "normales". También hay que desmentir el bulo de que la descarga de MP3 o vídeos en redes P2P es especialmente peligrosa desde el punto de vista de la seguridad e integridad de los sistemas (pero ésta es otra guerra).

Este incidente es un ejemplo más de que el ataque puede suceder en cualquier escenario y que por tanto la solución no es "demonizar" ciertos contenidos, sino que lo primordial es concienciar a los usuarios de que deben seguir unas normas básicas de seguridad para prevenir ser víctimas de este tipo de ataques automáticos.

Unas de esas normas básicas es que deben mantener sus sistemas puntualmente actualizados con los últimos parches de seguridad. Los usuarios de Windows que hubieran seguido esta sencilla regla y visitaron algunas de las 11.000 webs comprometidas, no sufrieron ninguna infección.

Navega por donde quieras, pero navega seguro.

Bernardo Quintero

09/07/2007 Los estafadores en Internet, más solidarios que nunca

Symantec publica una noticia que puede resultar chocante en un principio. Los estafadores en Internet donan parte del dinero conseguido con sus fraudes a proyectos de caridad. Es una tendencia que se está observado y que, aunque parezca extraño, tiene una explicación razonable.

La industria del malware y la estafa en Internet mueve un volumen importante de números de tarjetas de crédito, con los que trafican y de los que se benefician directa o indirectamente. En los ambientes adecuados, no es complicado conseguir números de tarjetas de crédito por algunas decenas de dólares. El "excedente" de información de algunas mafias es tal que, aparte de usarlos en beneficio propio, pueden permitirse el vender algunos números de tarjeta (con sus pins y códigos de seguridad adicionales), robados a través de phishing o malware.

La pregunta es: ante tanto número de tarjeta comprado y vendido, ¿cómo saber cuál es válido? ¿cuál se mantiene operativo y permite comprar realmente a través de la red? Comprobar la validez de los códigos de una tarjeta comprando cualquier producto puede hacer saltar las alarmas. Para un atacante que necesita pasar lo más inadvertido posible, las donaciones de caridad se han convertido en buenas aliadas

Los poseedores de los códigos robados traspasan pequeñas cantidades de dinero a páginas de caridad como por ejemplo, la Cruz Roja. Con esto se aseguran que, si la operación se realiza con éxito, la tarjeta puede volver a ser usada en compras más "lucrativas" o revendida. Existen otras ventajas, según Symantec. Los bancos pueden llegar a monitorizar las transacciones habituales de una tarjeta, y obtener un perfil de actuación "habitual" de su dueño. Donar cantidades a instituciones sin ánimo de lucro no es un movimiento "normal" para la mayoría de las personas, y precisamente ese carácter extraordinario lo hace pasar por movimiento perfectamente posible y ocasional para muchos. Sería complicado determinar si una donación concreta es "sospechosa" tanto en un usuario que la realice a menudo como para quien no lo tenga por norma.

Además, con este tipo de donaciones, voluntarias, pueden donar cantidades ridículas (desde algunos céntimos a un dólar) sin necesidad de comprar realmente nada y optimizar así los recursos invertidos en la comprobación real de la validez de la tarjeta.

El Washinton Post no opina que esto sea una nueva tendencia, y recuerda algunas situaciones similares anteriores. Hace dos años, las páginas que recolectaban donaciones para los damnificados por el Huracán Katrina ya obtuvo una buena inyección de dinero a través de este sistema. También recuerda que un administrador de una campaña presidencial en 2004 recibió durante varios días miles de pequeños pagos voluntarios (de cinco centavos) realizados con números de tarjeta distintos y automatizados a través de sistemas situados en Europa del este. Gracias a este "efecto colateral", recolectaron hasta 60.000 dólares que finalmente no pudieron quedarse.

Al menos, entre tanto tráfico de datos y dinero ganado de forma fraudulenta, reconforta saber que algunas ONG e instituciones de caridad sacan algún partido de esta "necesidad" de los estafadores... aunque a los dueños legítimos de las tarjetas seguro que no les hace ninguna gracia.

Sergio de los Santos

09/08/2007 Malware 2.0

Aunque no deja de ser una etiqueta de moda sin una definición clara, el concepto de la Web 2.0 hace referencia a una segunda generación de aplicaciones web dinámicas e interactivas donde el usuario tiene un mayor protagonismo y participación, frente a las webs estáticas tradicionales donde el usuario era un receptor pasivo. ¿Existe también un nueva generación de malware 2.0?

Tengo que confesar que creía que iba a ser original hablando del concepto Malware 2.0, pero una búsqueda en Google me ha sacado de mi error. Hace menos de un mes la empresa de seguridad PC Tools utilizó el término en una nota de prensa donde hablaba de una nueva generación de malware:

http://www.pctools.com/news/view/id/181/

PC Tools hace referencia a características que llevamos comentando tiempo atrás en Hispasec:

* La proliferación de nuevas variantes de malware ha crecido de forma brutal.

* Se utilizan técnicas automáticas para ofuscar las variantes y dificultar la identificación por firmas.

* La estrategia actual pasa por utilizar muchas variantes en vez de un único espécimen para llamar menos la atención y dificultar una respuesta rápida por parte de la comunidad antivirus (de ahí que llevemos bastante tiempo sin ver un gusano de propagación masiva como el ILoveYou y compañía).

A continuación, como era de esperar, utiliza este argumento para vender su producto antispyware, que utiliza técnicas adicionales para no depender en exclusiva de las firmas de detección.

Aunque esas características son una realidad evidente desde hace bastante tiempo, mi idea del concepto de Malware 2.0 tiene más analogía con la Web 2.0: el uso de la web como plataforma para la distribución, personalización del malware, y uso inteligente de los datos obtenidos por parte de los usuarios para propocionar "nuevos contenidos".

Para desarrollar la idea voy a utilizar un ejemplo de ataque real, de los muchos que están sucediendo a día de hoy, destinado a los usuarios de banca electrónica:

* Los atacantes diseñan un servidor web que hospeda el código malicioso.

* Para atraer a potenciales víctimas anuncian su URL a través de spam, en foros, comentarios en blogs, etc. con cualquier excusa (bien una noticia de actualidad, curiosidades, imágenes eróticas o cualquier otro contenido potencialmente atractivo que lleven a los usuarios a visitar el servidor web de los atacantes).

* Cuando un usuario accede al sitio de los atacantes, la web comprueba la versión del navegador del visitante y, si es vulnerable, devuelve un exploit específico para su versión del navegador que provoque la descarga automática y ejecución del troyano.

* Si el usuario tiene un navegador actualizado, utiliza la ingeniería social para que el usuario descargue y ejecute por si mismo el troyano (por ejemplo, mediante un ActiveX, decirle que es un vídeo, o una utilidad que requiere con cualquier excusa).

* Este primer troyano que se descarga es un "downloader", que lo que hace es instalarse en el sistema y descargar e instalar la última versión del troyano bancario, así como sucesivas actualizaciones que pudieran aparecer en el futuro.

* El troyano "downloader" también puede personalizar la versión del troyano bancario que descarga en función del sistema. Por ejemplo, si el usuario tiene una versión de Windows en español, el "downloader" instalará en el sistema un troyano bancario diseñado específicamente para entidades españolas.

* El troyano bancario puede estar destinado a unas entidades específicas o ser más genérico. En el caso de que tenga unas entidades predefinidas, si el usuario accede a las webs de banca electrónica reconocidas por el troyano, envía los usuarios y contraseñas de acceso del usuario al servidor web para que los atacantes puedan suplantar su identidad y realizar transferencias a otras cuentas.

* En el caso de un troyano bancario más genérico e inteligente, envía a un script del servidor web de los atacantes todas las URLs por las que el usuario navegue y que comiencen por https. En el servidor web tienen un listado de URLs de bancos, si alguna de las URLs que envía el troyano corresponde con el listado, entonces el servidor web devuelve al troyano una orden concreta: redirigir al usuario a un sitio de phishing de esa entidad, modificar en local la página web de la entidad para que pida la clave de operaciones, etc.

* La información de las URLs de páginas seguras (https) por la que los usuarios navegan, y que envían al servidor web, sirve a los atacantes para diseñar nuevos ataques y actualizaciones de su troyano bancario. Por ejemplo, imaginemos que en un principio los atacantes contemplaban a Banesto, pero no al BBVA. Los usuarios que visitaban la web de Banesto eran afectados, mientras que los del BBVA no porque el servidor web no devolvía ninguna orden concreta al no tener un ataque específico preparado. Los atacantes estudian periódicamente las estadísticas de las URLs que se centralizan en su servidor, y comprueban que hay muchos usuarios infectados que visitan la web del BBVA. Entonces deciden crear una nueva versión del troyano bancario específico o una página de phishing a la que redirigir a los usuarios infectados que la próxima vez visiten la web del BBVA.

Este último punto tiene cierta analogía con servicios web 2.0 como digg.com o meneame.net, si muchos usuarios visitan una página de un banco se contabiliza en el servidor de los atacantes como votos positivos y termina por aparecer en portada (en este caso en la lista negra de entidades para las que desarrollan un ataque concreto).

Cómo podemos ver, esta nueva generación de malware utiliza la infraestructura de la web para comunicarse con los sistemas infectados de los usuarios y realimentarse con la información que estos proporcionan, aprovechando esta inteligencia colectiva para ofrecer nuevos contenidos dinámicos en función de los perfiles de los usuarios. ¿Estamos ante el malware 2.0?

Bernardo Quintero

08/08/2007 Antivirus: rendimiento vs. protección

El mundo de los antivirus está en crisis técnica, que no comercial, sigue siendo un buen negocio. Pero a estas alturas a nadie escapa que los antivirus a duras penas logran tapar parte de la ventana de riesgo de infección a la que todo usuario de Windows se expone en Internet. Ante este panorama cabría pensar que están triunfando los antivirus que mayor protección ofrecen, si bien la realidad es distinta.

La gran proliferación y diversificación del malware ha puesto en jaque a un esquema basado en tener fichados a los malos: firmas para identificar al malware conocido, firmas genéricas para identificar variantes de una misma familia, y heurísticas basadas en la detección de código sospechoso.

Los malos han ganado la partida en este juego. Modifican una y otra vez el código para que las firmas y heurísticas existentes no puedan detectarlos, cambian la cara de sus especímenes para evitar ser reconocidos aunque en el fondo siguen haciendo el mismo daño. Lo hacen de forma tan masiva que los antivirus a duras penas pueden seguir el ritmo para actualizarse, no dan a basto, están saturados. Es una carrera sin final y nos llevan mucha ventaja.

Hay que cambiar de estrategia. Visto que actualizar firmas de forma constante no es suficiente, los antivirus han optado por implementar nuevas tecnologías que les permita más proactividad. El fin es poder detectar el malware nuevo, desconocido o variante. No depender de una firma reactiva, ser más genéricos y proactivos en la protección.

Son varias las empresas antivirus que han arriesgado en ese campo, incorporando nuevas tecnologías y capas de seguridad al motor antivirus tradicional, que dotan a la solución de un mayor poder de protección. Pero no todos son ventajas a la vista del usuario, la incorporación de este tipo de tecnologías adicionales suele conllevar también un software más “pesado”, que consume más recursos, enlentece el sistema, tiende a dar más falsos positivos y/o termina haciendo preguntas incomodas al usuario:

“El proceso svchost.exe intenta conectar a Internet. ¿Permitir o denegar?”

¿No se supone que el antivirus debe saber si es algo peligroso o no?, ¿por qué me pregunta a mí?. Después de una serie de pensamientos similares, el usuario acabará por tomar alguna decisión del tipo:

.Intentará averiguar en google que es “svchost.exe” (no llegará a ninguna conclusión, y a la segunda o tercera pregunta sobre otros procesos desistirá en la búsqueda de la verdad)

.Permitir Todo (tarde o temprano terminará infectándose)

.Denegar Todo (dejará de funcionarle algún software legítimo)

.Desinstalar el antivirus e instalar otro que no le haga perder tiempo con ventanitas emergentes y preguntas

que no sabe contestar (sin excluir las decisiones anteriores, el usuario suele terminar desembocando en este punto y cambiando de antivirus)

Percepción del usuario

Ahora tenemos a un usuario con un antivirus tradicional, basado en firmas, que no incluye tecnologías adicionales, que no enlentece el arranque de su sistema, que no le consume mucha memoria, que no le importuna con preguntas... tenemos a un usuario menos protegido, pero un usuario que está teniendo una "buena experiencia" con su antivirus.

Y es que aunque teóricamente un desarrollador antivirus debe balancear entre rendimiento y protección, la realidad es que el usuario sólo puede percibir el rendimiento. Un usuario no sabe de tecnologías, un usuario no puede evaluar el grado de protección que le ofrece una solución, en la lógica de un usuario un antivirus debe protegerle de infecciones y punto.

En los años 90 cuando un virus infectaba el ordenador se notaba de inmediato: borraba archivos, mostraba imágenes en pantalla, etc. Cuando un usuario se veía infectado por un virus aun teniendo antivirus, motivaba el cambio de producto: "este antivirus no es bueno, ha permitido que me infecte". Pero ahora el panorama es bien diferente, el malware de hoy día está diseñado para permanecer oculto y el mayor tiempo en los sistemas infectados, sin dar señales de vida. Así que el usuario seguirá con la buena experiencia de su "antivirus ligero" pese a que su sistema esté infectado. Simplemente, el usuario no se entera.

Lo que si va a notar un usuario de inmediato es si el antivirus interfiere en su sistema y en el trabajo diario. Esa experiencia que si puede percibir de forma directa es la que decanta hoy día la evaluación de un antivirus y la elección final por parte del usuario.

La balanza por parte del usuario está inclinada claramente hacia un lado: el rendimiento. Mientras que algunos antivirus son conscientes de ello y explotan esta visibilidad parcial por parte de los usuarios para ganar mercado, otros siguen intentando equilibrar la balanza, o dándole más peso a la protección, y perdiendo clientes en el camino.

¿Deben las empresas antivirus renunciar a ofrecer una mejor protección? Evidentemente no, pero la experiencia del usuario debe ser un objetivo igual o más importante si cabe, incluso en muchas ocasiones tendrá mayor peso. De nada sirve diseñar el antivirus más seguro si los usuarios no lo pueden utilizar. Para el usuario el mejor antivirus no es el más seguro, sino el más confortable.

Algunos ejemplos

La pregunta sobre el svchost.exe me saltó ayer mientras probaba un antivirus, y no fue la única pregunta que hizo. Es más, después de instalarse, tras el primer reinicio del sistema, hizo un análisis completo de todos los archivos del disco duro en segundo plano. Por la actividad del disco duro deduje lo que estaba haciendo, y haciendo doble click en el icono del antivirus pude confirmarlo en la ventana del escaner.

Como medida de seguridad estaba muy bien, pero, ¿cuál es la experiencia de un usuario común? Pues no tiene dudas, tras instalar el antivirus el sistema se ha vuelto muy lento y apenas lo deja trabajar. El usuario no sabe que es una acción que llevará a cabo sólo en el primer reinicio y no en posteriores, la percepción es que instalando el antivirus X el sistema inmediatamente se vuelve lento.

¿Por qué el antivirus no deja el análisis de todos los archivos para más tarde, cuando detecte que el sistema

lleva un tiempo en "reposo" en vez de hacerlo justo en el inicio? Incluso podría pausar ese análisis en segundo plano si detecta que el usuario comienza a utilizar el ordenador, o al menos regular la velocidad y consumo de recursos del análisis para no interferir la actividad del usuario.

Probando otros antivirus se puede notar claramente el cambio de enfoque, acertado desde el punto de vista comercial, explotando al máximo los conceptos de velocidad y rendimiento. Aunque en ocasiones sea a costa de una menor protección o simplemente aplicando cierta picaresca.

Hay un antivirus que se vende como uno de los más rápidos, para ello tiene una opción por defecto de análisis a demanda donde no utiliza las técnicas de heurística que más recursos consume, con las que hacen las pruebas de velocidad. Cuando toca hacer una prueba de detección, piden encarecidamente que se utilice la opción con la heurística más lenta activada. Objetivo: aparecer en las evaluaciones como el más rápido sin perder capacidad de detección. Lo logran.

Resumiendo

Demostrar que una tecnología antivirus ofrece mejor protección que otra es complicado. Desde el punto de vista de marketing el usuario está cansado, al fin y al cabo todos los antivirus afirman ser los mejores, y se deja llevar por la propia experiencia o por terceros confiables creadores de opinión.

La experiencia del usuario tiene una visibilidad muy parcial, no puede saber que grado de protección real le ofrece un producto. Se dejará llevar por indicadores tales como la no interferencia con su trabajo y el rendimiento del sistema. El usuario no sabe si está infectado o no, pero si sabe si el antivirus le molesta.

Los terceros confiables no son confiables. La dificultad que el usuario tiene para evaluar el grado de protección de un antivirus también se traslada a los creadores de opinión, desde foros de Internet pasando por revistas de informática y comparativas que tampoco están diseñadas para evaluar las nuevas tecnologías. También tienen la resposabilidad de explicar cual es la situación actual y las diferencias entre tecnologías, hay que formar a los usuarios.

Los evaluadores de antivirus deben evolucionar a nuevas metodologías, siguen (seguimos) utilizando tests de los años 90 dando resultados adulterados y penalizando a las nuevas tecnologías. Son las fuentes de la que beben los terceros confiables, "culpables" también de la formación en nuevas tecnologías que requieren traducir su eficacia real en indicadores que a día de hoy simplemente no se miden.

Los desarrolladores antivirus deben reinventarse y no perder el foco sobre el usuario. Hay productos que están incorporando tecnología sobre tecnología en su búsqueda de minimizar la ventana de riesgo de infección, pero convirtiéndose en un software complejo, poco optimizado, que consume muchos recursos, y que ofrece una pobre experiencia al usuario.

Hay que evolucionar, pero no a cualquier precio. A veces tendemos a ofuscarnos con soluciones técnicas y olvidamos que al final un usuario, que no es informático ni tiene nociones de seguridad, tendrá que convivir con esas soluciones en su día a día en un PC normal, no sobrado de recursos, que ejecuta otras aplicaciones que son realmente las importantes para él.

Bernardo Quintero

18/08/2007 El escarabajo de oro

La lectura de "El escarabajo de oro", relato de Edgar Allan Poe, ha supuesto para muchos el bautismo con el criptoanálisis, descubriendo uno de los métodos básicos para romper un mensaje cifrado y recuperar la información original.

Edgar Allan Poe es tal vez más conocido por sus obras de misterio e historias macabras, si bien también fue un apasionado de la criptografía. Esa afición ha quedado reflejada para la posteridad con mensajes ocultos en varios de sus poemas y de forma más explícita en "El escarabajo de oro".

Esa faceta se hizo aun más patente cuando en 1839 comenzó a escribir en la publicación Alexander's Weekly Messenger una serie de artículos sobre criptografía, llegando a retar a sus lectores a que le enviaran mensajes cifrados que él intentaría resolver.

Su colaboración con la publicación apenas duró 5 meses. Un año más tarde comenzó de nuevo a escribir sobre criptografía en la publicación Graham's Magazine, bajo el título "A Few Words on Secret Writing" y una serie de tres artículos. En esta publicación afirmó que durante el transcurso del anterior reto logró resolver todos los mensajes cifrados enviados por los lectores de Messenger, aproximadamente unos cien.

Según Poe, recibió dos nuevos mensajes cifrados de un lector, Mr. W.B. Tyler, que reprodujo en Graham's Magazine para animar a sus lectores a que intentaran descifrarlos. Poe afirmó que no había podido resolverlos por falta de tiempo. Siempre se tuvo la sospecha de que la historia era una excusa, y que Tyler era en realidad Poe, que habría dejado de esta forma algún mensaje oculto para la posteridad.

El primero de los mensaje cifrados de Tyler no fue resuelto hasta pasados más de 150 años, en 1992, por Terence Whalen, un estudioso de la obra de Poe, que a día de hoy ejerce en la universidad de Illinois.

Este primer mensaje resultó ser un fragmento de "Cato", obra de Joseph Addison que data de 1713, y que a priori no establece relación alguna con Poe. En cuanto al sistema de cifrado utilizado, tampoco resultó ser nada sofisticado, se trataba de una simple sustitución monoalfabética, que podía ser resuelta de forma similar a como se describe en "El escarabajo de oro".

El segundo mensaje cifrado de Tyler seguía resistiendose. En 1996, Shawn J Rosenheim, profesor del Williams College y estudioso de Poe, anunció un concurso por el que premiaría con 2.500 dólares a la persona que descifrara el segundo mensaje de Tyler.

En el año 2000 Gil Broza, actualmente consultor IT, se alzaría con el premio al resolver el segundo mensaje de Tyler con la ayuda de un ordenador, varios programas que diseñó para la ocasión, y dos meses de quebraderos de cabeza. El texto descifrado resultó ser de lo más decepcionante, ya que no se ha establecido su autoría y a priori no guarda relación alguna con Poe. Aun así, continúan las teorías sobre que Poe pudiera ser el autor de estos mensajes cifrados y que, una vez descifrados, aun pudiera contener algún mensaje oculto que aun no habría sido interpretado.

Si has llegado hasta aquí y no conocías la obra de Poe o te has interesado por el criptoanálisis, tal vez te apetezca leer "El escarabajo de oro":

http://www.librosgratisweb.com/pdf/poe-edgar-alan/el-escarabajo-de-oro.pdf
http://www.estadisticaparatodos.es/taller/criptografia/Edgar_Allan_Poe-El_Escarabajo_de_ oro.pdf

(HTML) http://es.wikisource.org/wiki/El_escarabajo_de_oro

Bernardo Quintero

17/10/2007 ¿Es la Russian Business Network el centro de operaciones mundial del malware?

Brian Krebs publica una serie de interesantes artículos sobre la Russian Business Network (más conocida como la RBN), una compañía que supuestamente proporciona alojamiento e infraestructura web a la creciente industria del malware, convirtiéndose así en una especie de centro de operaciones mundial desde donde se descargan los troyanos y hacia donde viaja la información robada.

La RBN se encuentra en St. Petersburg y proporciona alojamiento web. Su actividad parece estar íntimamente relacionada con la industria del malware, hasta el punto de que muchos han decidido bloquear directamente toda conexión con direcciones pertenecientes a esta red. Y no sólo malware. Se dice que la mitad del phishing mundial está alojado impunemente en alguno de sus servidores.

En los últimos años no es fácil encontrar un incidente criminal a gran escala en la que no aparezcan por algún sitio las siglas RBN (o “TooCoin” o “ValueDot”, nombres anteriores con los que ha sido conocida). En 2005 se estaba aprovechando de forma masiva una vulnerabilidad en Internet Explorer para instalar un keylogger. Se demostró que la mayoría de datos robados iban a parar a un servidor de la RBN. Los servidores de la RBN estaban detrás del incidente contra la HostGator en 2006. Aprovechando un fallo en Cpanel, consiguieron tener acceso a cientos de webs de la compañía. En 2007, la empresa de hosting gratuito IPOWER también fue atacada y se instalaron en sus páginas “frames” que de forma transparente redirigían a sitios en la RBN donde se intentaban instalar troyanos. Malware como Gozi, Grab, Metaphisher, Ordergun, Pinch, Rustock, Snatch, Torpig... todos se han servido de los servidores de la RBN para “alojarse” o alojar datos. Los ejemplos son muchos y variados. Mpack la herramienta usada en varios ataques masivos durante 2007, es vendida desde uno de los servidores de la RBN.

Ante tanta evidencia, son muchos los administradores que han decidido bloquear por completo el acceso a los servidores alojados en la RBN. Pero no ha servido de mucho. Han aprendido a enrutar las conexiones a través de otras webs comprometidas en Estados Unidos y Europa de forma que, aunque sea dando un rodeo a través de otras IPs (habitualmente usuarios residenciales troyanizados o webs atacadas), siguen operando de forma normal. Por ejemplo, en el reciente ataque al Banco de la India, al seguir el rastro del malware que se intentaba instalar en los sistemas Windows que visitaban la web, se observó que tras pasar la información a través de varios servidores, finalmente acababa en un servidor de la RBN.

Tras las acusaciones publicadas en el Washinton Post, un tal Tim Jaret que decía pertenecer a la RBN lo negaba todo. Decía que no podía entender por qué se le acusaba basándose en suposiciones. El tal Jaret incluso se queja de que intentó colaborar con el grupo antispam Spamhaus (que tiene continuamente bloqueadas nada menos que más de 2.000 direcciones IP de la RBN clasificadas como origen de correo basura) sin éxito.

En SANS Internet Storm Center tienen una clara opinión al respecto, no van a tirar piedras sobre su tejado. Y es que según Verisign, la RBN cobra hasta 600 dólares mensuales por un alojamiento “a prueba de balas” lo que en este caso significa que no cederá a presiones legales ni será cerrado por muy inapropiado o “infeccioso” que sea su contenido. Aun así, el tal Jaret afirma que la RBN tiene el nivel de

“criminalidad” habitual en cualquier proveedor web, y que habitualmente cierra las webs en menos de 24 horas, facilitando el trabajo a los profesionales de la seguridad. Sin embargo, es posible que la única acción de la RBN cuando recibe presiones para cerrar un sitio web, sea aumentar el “alquiler” a los delincuentes que se basan en ella para operar.

Por último, se le pidió al tal Jaret que ofreciera nombres de usuarios legítimos de sus redes, y contestó que razones legales se lo impedían.

La RBN (rusa, cómo la gran escuela creadora del malware 2.0) se ha convertido así en cómplice y centro de operaciones web para la industria del malware, que encuentra un aliado que sabe mantener la boca cerrada y las manos quietas si se le paga lo suficiente. Symantec lo llama “el refugio para todo tipo de actividades ilegales en la Red”.

Por si queda alguna duda sobre su intención de permanecer “anónimos”, basta con comprobar hacia qué IP apunta su dominio principal rbnnetwork.com

Sergio de los Santos

02/11/2007 Ataque con troyano para usuarios de Mac

Detectada diversas variantes de un troyano destinado a usuarios de Mac. De momento se ha detectado únicamente hospedado en páginas de contenido pornográfico, a través de las cuales intentan engañar a los usuarios para que se instalen el troyano.

Se trata de un ataque dirigido a usuarios de Windows y Mac desde páginas con supuestos vídeos pornográficos. Para atraer a las potenciales víctimas, las direcciones de las webs que contienen los troyanos han sido anunciadas a través de spam, incluyendo el envío de los enlaces a varios foros de usuarios de Mac.

Cuando el usuario visita una de las páginas y selecciona visualizar uno de los vídeos, el servidor web detecta si el sistema es un Windows o Mac a través del user-agent del navegador. En función de ese dato, la página web intentará que el usuario se instale la versión del troyano para Windows (extensión .exe) o para Mac (extensión .dmg).

La estrategia de los atacantes consiste en hacer creer al usuario que necesita instalar un componente adicional, un codec, para poder visualizar el vídeo. El usuario de Mac tendrá que introducir la contraseña de administrador para proceder a la instalación del troyano, si bien muchos podrían hacerlo creyendo que es necesario para instalar el componente que les permitirá ver el deseado vídeo.

Una vez el troyano se instala lleva a cabo su cometido, que no es otro que modificar los servidores DNS del sistema para que apunten a unos nuevos que están bajo el dominio de los atacantes. Estos servidores DNS llevarían a cabo un ataque del tipo pharming, ya que pueden redireccionar ciertos dominios, como el de algunas entidades bancarias, a servidores que hospedan phishing con el fin de sustraer las credenciales de acceso de las víctimas.

La detección antivirus es de momento escasa, normal si tenemos en cuenta que el malware suele ser, en la práctica, un terreno de Windows, en incluso muchas casas antivirus no tienen soluciones para Mac. Las diversas variantes a las que tenemos acceso en Hispasec hasta el momento son detectadas por ninguno,

uno, o a lo máximo dos productos antivirus, entre los que se encuentra Sophos que lo identifica con el nombre de "OSX/RSPlug-A" y Mcafee como "OSX/Pupe".

La recomendación obvia a los usuarios de Mac es que no instalen ningún software de fuentes no confiables y, dado este caso en concreto, especialmente desconfíen de cualquier web de contenido adulto que les incite a instalar un supuesto codec de vídeo.
Aunque el ataque también se dirige a usuarios de Windows, que es lo común, la noticia es que se hayan molestado en desarrollar una versión del troyano específica para los usuarios de Mac. Hasta la fecha la mayoría del malware para Mac era anecdótico, pruebas de concepto o laboratorio, que realmente no tenían una repercusión significativa entre los usuarios de Mac. En esta ocasión estamos ante un caso real de malware funcional desarrollado por atacantes que han fijado, como parte de sus objetivos, el fraude online a usuarios de Mac.

¿Caso puntual o el comienzo de una nueva era en lo que respecta al malware para Mac?

Más información y ejemplos de las webs que distribuyen el troyano pueden encontrarse en el blog del laboratorio de Hispasec:
http://blog.hispasec.com/laboratorio/250

Bernardo Quintero

05/12/2007 Servicios antiphishing ¿efectivos?

Un estudio de Symantec revela que el 25% de las visitas a un sitio de phishing se produce durante la primera hora del lanzamiento del fraude. Transcurridas 12 horas habrá recibido el 60% de las visitas. Si los servicios antiphishing tardan más tiempo en desactivarlos, ¿cuál es su efectividad real en la prevención del fraude?

El estudio, que se ha llevado a cabo durante varios meses, analiza los logs correspondientes a 6.158 ataques, y pone números a algo que todos sabíamos: en un fraude por phishing las primeras horas son cruciales y concentran el mayor porcentaje de las visitas y estafas.

Durante las 6 primeras horas del ataque se llegarían a concentrar el 51,6% de las visitas, entre las 6 y 12 horas aumenta un 10,7%, entre las 12 y 24 horas se suma un 13%, y el 24,6% de las visitas restantes se suceden transcurridas las primeras 24 horas.

Estos datos dejan en entredicho la efectividad de los servicios antiphishing reactivos que mantienen medias superiores a las 6 horas de cierre, ya que no evitarían la mayoría de las visitas y por tanto la rentabilidad del ataque. Esto explica en parte que, pese a la inversión en este tipo de servicios, los ataques a ciertas entidades sigan siendo periódicos.

Desde el punto de vista del atacante, un servicio antiphishing de una entidad que cierre en el menor tiempo posible repercutiría negativamente en su negocio, y por tanto es de preveer que migrara sus ataques a otras entidades que no entorpecieran tanto el fraude.

Por ello la velocidad en el cierre de las infraestructuras de phishing es crucial en la prevención, tanto por los casos puntuales, como por estrategia a medio plazo que conlleve una disminución en los ataques a una entidad al dejar de ser un objetivo rentable.

¿Deberían las entidades exigir tiempos de reacción a los servicios antiphishing?

Queda claro que a mayor tiempo de reacción aumenta la rentabilidad del atacante, lo que también favorecería que la entidad sufra nuevos ataques. Como efecto colateral la empresa que ofrece el servicio antiphishing tendría que llevar a cabo más actuaciones, y también saldría beneficiada económicamente. Algo falla en la ecuación.

Dada la importancia de la velocidad de reacción, es lógico pensar que la entidad requiriera establecer algún tipo de escala basada en tiempos. No debería pagar lo mismo por la desactivación de un phishing en 1 hora que en 24, debería incentivar y premiar la mayor celeridad posible en las actuaciones, inclusive no pagar aquellas que se dilaten demasiado en el tiempo.

La realidad es que el cierre de una infraestructura de phishing depende de factores externos que no puede controlar la empresa de seguridad, y por lo tanto la efectividad en casos concretos, o en determinadas campañas, puede ser muy variable. No obstante, eso no debe ser ápice para que se establezcan mecanismos que incentiven los mejores resultados.

De los últimos 100 casos de phishing gestionados por el servicio antifraude de Hispasec, 47 de ellos se cerraron en menos de 1 hora. La media de cierre se sitúa en 3 horas 1 minuto.

Bernardo Quintero

Entrevista


Eugene Kaspersky

En poco más de una década, **Eugene Kaspersky** ha construido una de las empresas antivirus más respetadas entre los profesionales del sector. Kaspersky se caracteriza por ser un profesional al que le apasiona su trabajo. Su empresa dice y hace lo que quiere, que no siempre tiene por qué ser políticamente correcto... aunque sí que parece acertado la mayor parte de las veces.

Hispasec: ¿Cómo surge la idea de crear una empresa antivirus?

Eugene Kaspersky: Comencé a trabajar como “cazador de virus” profesional a principios de los 90, cuando acabé el servicio militar y me uní a KAMI, una de las compañías de IT más grandes del momento en Rusia. Recibíamos financiación de la compañía, y eso me permitió investigar y crear un equipo de expertos de perfil alto que todavía forman parte de la empresa.

Sin embargo en 1997 KAMI decidió abandonar el desarrollo de software y concentrarse en la integración de sistemas. No queríamos cerrar nuestro proyecto antivirus, así que la única opción que nos quedaba era fundar nuestra propia compañía, lo que hicimos en 1997. En ese momento nadie quería invertir en nuestro negocio ni darnos créditos, éramos muy pequeños y desconocidos. Y hasta hoy no hemos tenido ningún inversor ni pedido ningún préstamo. Ahora somos los suficientemente grandes para financiar nuestro negocio y desarrollar nuestro proyecto.

H: En Hispasec realizamos varias comparativas antivirus para revistas del sector a finales de los años 90. Una de las pruebas consistía en enviar de forma anónima un malware nuevo

a los laboratorios para ver el tiempo de reacción y la calidad de la respuesta. Recordamos con agrado la anécdota de que durante alguna de esas pruebas analizaste la muestra y contestaste personalmente al ficticio usuario infectado. ¿Cómo compaginabas tu puesto de presidente de una empresa en expansión con la dedicación al análisis de malware y soporte a los usuarios?

EK: "Finales de los 90" fue hace 10 años... en ese momento yo estaba realmente trabajando parcialmente como analista de virus, observando las peticiones de los usuarios, analizando ficheros sospechosos, añadiendo nuevos registros... Comencé a delegar más obligaciones en otros entre 2003 y 2005, cuando emergieron más y mejores investigadores en nuestro laboratorio que hacían el trabajo igual de bien o mejor que yo. Finalmente reconocí que realmente no me necesitaban en la línea de decisiones. Así que lentamente dejé el trabajo diario de análisis y ahora más que nada me centro en la estrategia de la compañía e innovaciones tecnológicas. Viajo también mucho más para estar más en contacto con la realidad.

H: Siguiendo con aquella anécdota, en la respuesta que recibimos apreciábamos un trabajo artesanal. Realmente habías analizado la muestra y, además de la actualización para desinfección, nos dabas detalles del funcionamiento interno del malware. Con el volumen actual de malware es impensable que se pueda continuar haciendo un trabajo tan artesanal en los laboratorios y se intuye que buena parte del proceso de análisis se encuentra automatizado. A lo largo de estos años, ¿cómo ha ido evolucionando el trabajo en los laboratorios antivirus? ¿cuáles son los retos actuales y cómo se abordan?

EK: Por supuesto, la mayoría del trabajo está automatizado, pero la recoleción de muetras también, así que no necesitamos responder a cada muestra añadida a la colección. Contestamos a las peticiones "humanas" solo.

H: La mayor parte del malware de hoy día forma parte de un negocio criminal, podríamos decir que se ha profesionalizado la antigua figura del creador de virus. Atrás quedan los virus que infectaban ejecutables y vivimos una auténtica avalancha de malware estático, como troyanos o adware. Parece que también existe una automatización en la creación de malware, con miles de variantes que tienen el mismo objetivo y sólo buscan evitar la detección de los antivirus. ¿Qué diferencias claves encuentras entre el malware de 1998 y el del 2008? ¿Crees que volverán a tener un boom los virus infectores y polimórficos? De suceder eso, ¿crees que algunas soluciones antivirus actuales se han acostumbrado al malware estático y tendrían problemas para adaptarse a ese nuevo escenario?

EK: En realidad hoy en día afrontamos más y más infectores y malware polimórfico, especialmente "polifórmico en web". Así que a finales de los 90 los infectores le cedieron la cuota de mercado al malware estático. No lo recuperan (todavía hay cientos de veces más malware estático), pero cada vez estamos recibiendo más malware de última generación.

H: En la actualidad, ¿cuál es tú función en Kaspersky Labs? ¿Sigues realizando tanto labores de gestión como técnicas?

EK: Nunca he sido un manager directo, del día a día. Prefería tener un buen equipo de managers que tuvieran la capacidad y libertad de hacerlo bien por ellos mismos. Mi trabajo es más que nada comprender "el cuadro", desarrollar la estrategia de la compañía, tomar parte en el marketing del producto, innovaciones tecnologicas y representar a la compañía.

HS: Kaspersky siempre ha tenido fama de buen motor antivirus en foros técnicos, sin embargo el ranking de ventas suele estar liderado por otras marcas. ¿Cree que la decisión de los usuarios finales se deja llevar más por el marketing que por la realidad del producto? ¿Qué debería tener en cuenta el usuario a la hora de elegir su antivirus? ¿Existe una fuente confiable donde pueda comparar?

EK: La razón por la que no estamos en la las compañías “BigThree” es muy simple: cuando fundamos nuestra compañía independiente, cuando empezamos a explorar el mercado, otros ya llevaban allí muchos años, y no había espacio libre para nosotros. Así que tuvimos que luchar por nuestro espacio durante años, explicando nuestra posición y promocionando nuestra tecnología, productos y servicios. Por eso en algunos países (no todos) somos valorados solo por usuarios avanzados, y menos reconocidos por la mayoría del mercado. Pero eso está cambiando.

H: En el escenario actual, con un volumen de malware muy considerable y distribuido, ¿tiene sentido seguir manteniendo la lista In-The-Wild y utilizarla como referencia para evaluar los antivirus?

EK: Por supuesto que no. Porque no es posible aguantar una lista “in the wild” si salen miles de nuevos malware cada día. Todas deberían estar ITW. Así que tenemos que cambiar esta metodología, pero no es una tarea fácil.

H: ¿Qué opinión te merece VirusTotal y cuál crees que debe ser su evolución y papel en la industria antimalware?

EK: Este tipo de servicios son una herramienta para usuarios de Internet experimentados, y resultan un servicio poderoso para recolectar malware en la Red.

H: Al margen de Kaspersky Labs, ¿a qué dedicas más tiempo últimamente? ¿Hobbies?

EK: ¿Hobbies? Llevar una compañía exitosa de ITTP (IT Threat Prevention) , hacerla crecer con cero ingresos (con la ayuda de otros) explicar amenazas, solucionar problemas... ¿acaso alguien necesita otro hobbie aparte de eso?

EK: ¿Alguna predicción en materia de seguridad informática? ¿Qué nos espera?

EK: Estoy esperando que los gobiernos presten más atención a los problemas de seguridad de la red global. Identificación personal, una Internet-Interpol realmente internacional nos traerá más regulaciones y restricciones. Sólo eso puede hacer disminuir la carga de malware en Internet. Si no hacemos eso... ¿Cuánto tráfico parasitario transfiere Internet? ¿Cuántos terawatios desperdiciamos por eso? ¿Cuántas centrales eléctricas trabajan sólo para soportar el crimen electrónico? ¿Cuánta electricidad, centrales de datos, canales... necesitaremos en 5, 10, 20 años si el crecimiento del malware se mantiene al mismo nivel?

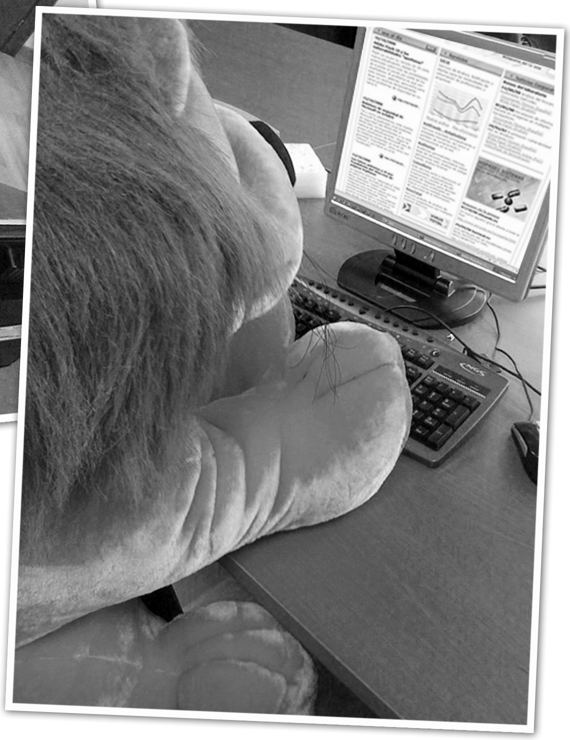
H: Un libro, una canción.

EK: Muchos. Puedes encontrar la información en www.kasperskyclub.com



Empleado del año





Capítulo 10

AÑO 2008

7D8

3730

11111011000



1247443200 – 1278979199



Durante este año...

_ En enero se registra una caída del Ibex 35 del 7,54%, retrocediendo hasta los 12.625 puntos. Aunque se recuperaría ligeramente, **la crisis es ya palpable**. En septiembre bajaría de 11.000 puntos. En octubre el Ibex-35 sufre la peor caída de su historia, un 9,14% y retrocede hasta los 8.997,7

_ En febrero **Fidel Castro** renuncia al cargo por motivos de salud, después de 49 años en el poder.

_ En las elecciones generales de España, el **PSOE revalida título**. Se crearía una pequeña crisis en el principal partido de la oposición.

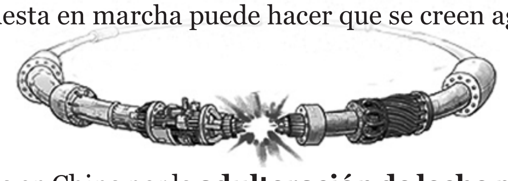
_ La sonda estadounidense **Phoenix** aterriza en Marte. Meses después podría usar su micrófono para oír los primeros sonidos del planeta rojo.

_ Del 14 de junio al 14 de septiembre se celebra la **Exposición Internacional de Zaragoza** (conocida como Expo Zaragoza 08), bajo el lema "Agua y desarrollo sostenible". No gozaría del éxito y popularidad de la Expo'92 de Sevilla.

_ En junio Barack Obama se convierte en el primer candidato negro a la presidencia de Estados Unidos, tras una reñida campaña contra la también demócrata Hillary Clinton.

El 20 de agosto, el vuelo 5022 de la compañía **Spanair**, se estrella poco después del intento frustrado de despegue. Mueren 154 personas. El vuelo sufre algunos problemas técnicos antes de despegar, pero aún así, lo intenta. Se barajan todo tipo de teorías sobre las verdaderas causas del desastre. Las tareas de identificación de cadáveres duran más de lo previsto. Durante los juegos olímpicos de Pekín, algunos españoles lucen crespones negros en sus brazos para mostrar solidaridad con las víctimas del accidente, aun siendo una manifestación no apoyada por el COI (Comité Olímpico Internacional) no son sancionados. El 24 de agosto se estrella en Kirguistán, al aterrizar, el vuelo 6895 de la compañía Itek-Air, mueren 69 personas.

_ Comienza a funcionar el 10 de septiembre en Suiza el acelerador de partículas **LHC (Large Hadron Collider)**. Se pretende hacer colisionar partículas subatómicas a grandes velocidades para simular algunos eventos ocurridos durante o inmediatamente después del "big bang". Algunas voces de supuestos científicos adelantan que su puesta en marcha puede hacer que se creen agujeros negros y provocar el fin del planeta.



_ En septiembre salta la alarma en China por la **adulteración de leche para bebés**, en la que se detecta melamina. Esta sustancia es agregada a los lácteos para que, en los controles, parezcan tener un mayor contenido en proteínas que el real. La sustancia resulta tóxica para el ser humano. Cuatro bebés mueren en

China, y otros miles quedan gravemente intoxicados. Se acusa al gobierno Chino de ocultar la información hasta que hubiesen terminado los juegos olímpicos de Pekín de agosto para no dar mala imagen. Los chinos acuden en masa a países vecinos a comprar leche, que debe ser racionada. Se detectarían partidas de este tipo de leche en España.

_ El **SIMO se cancela** debido a la crisis. La Feria Internacional de Informática, Multimedia y Telecomunicaciones no celebra su 48º edición tras el anuncio de las grandes empresas del sector de que no acudirán al encuentro.

_ El 26 de septiembre **muere Paul Newman**, el gran actor americano nacido en 1925.

_ El 28 de septiembre, la **SpaceX Falcon 1** es el primer vehículo espacial desarrollado de forma privada que es lanzado en órbita.

_ En octubre la crisis continúa. George W. Bush firma el plan de emergencia de estabilización de la economía, creando de la nada **700 mil millones de dólares** para comprar activos bancarios.

_ El 4 de noviembre **Barack Obama es elegido presidente** en las elecciones generales de Estados Unidos. Es el primer presidente afroamericano en la historia del país, y se entiende como un cambio radical tras la criticada gestión de su predecesor George W. Bush. Obama realiza una exitosa campaña de marketing a través de Facebook, atrayendo a los jóvenes que buscan el cambio con las redes sociales y las nuevas tecnologías. Su rival en las elecciones, John McCain, sigue una campaña de captación de voto tradicional mucho más cara y, como se demostraría, no tan efectiva como la de Obama. Poco después materializaría varias promesas electorales, que consistían básicamente en deshacer el camino hacia la guerra iniciado por Bush.

_ Durante noviembre, se intensifica el debate sobre **la necesidad de regulación profesional de la Informática en España**. Se convocan varias manifestaciones.

_ A principios de diciembre se producen **revueltas en Grecia**, a causa de la muerte de un adolescente de 15 años por un disparo de las fuerzas especiales de la policía griega.

_ Se añade **un segundo extra al año** el día 31 de diciembre.

Seguridad Informática



_ **Se elimina la opción de "no-distribución" en VirusTotal**. Bernardo Quintero ofrece una amplia explicación de los motivos en el blog de VirusTotal, en inglés, y se disculpa por los usuarios legítimos de esta opción. Sin duda, es en los comentarios de esta entrada en inglés donde más se insulta a Hispasec en general y a familiares de muchos en particular por el hecho de eliminarla. Esta opción permitía el envío a VirusTotal.com de una muestra sin que esta fuese reportada de forma automática a las casas antivirus, aun si era clasificada como malware por algún motor. Aunque se afirma y (se hace) que se pueden plantear soluciones para quien específicamente lo requiera, muchos prefieren abandonar el uso del servicio no sin antes manifestarlo públicamente en comentarios en el blog. La reacción en España es mucho menos impactante. Afortunadamente, la carga y uso de VirusTotal.com no se resiente, es más, aumenta.

_ Se encuentra la enésima vulnerabilidad que permite la ejecución de código en **RealPlayer**. Es explotada antes de que exista solución. Los atacantes se cuelan en servidores que alojan páginas e incrustan sus propios IFRAMEs para infectar a los visitantes. Se estima que existen unas 80.000 páginas legítimas alteradas con exploits para este fallo que permiten aprovechar la vulnerabilidad e instalar algún tipo de malware. Todo tipo de webs se ven afectadas por este problema: desde gobiernos a grandes empresas pasando por bancos.

_ La empresa Sentrigo publica una encuesta sobre seguridad en **Oracle**. Los resultados materializan la sensación generalizada del problema de la gestión de seguridad de Oracle. Dos tercios de los administradores **no parchean** sus bases de datos.

El **grupo 29A anuncia oficialmente su retirada**. Se trata un síntoma más de que hace ya tiempo se terminó la época romántica de la creación de virus. Representaron la élite en cuanto a creación de virus se refiere, era realmente un laboratorio de I+D en España. De marcado carácter underground (29A es 666 en hexadecimal) mantuvieron un altísimo nivel de VirusCoding desde su creación con especímenes que innovaron en su momento en el mundo de la codificación vírica. Sus miembros desarrollaron los troyanos más punteros de la época, por ejemplo, aprovechando Internet cuando no era tan habitual estar conectado a la red. Entre otros, programaron el virus HPS, que levantó polémica por ser el primer virus polimórfico diseñado para Windows 98.



En realidad se trataba de un virus creado para obtener la atención de los medios, puesto que deliberadamente comprobaba al inicio de su ejecución la versión del sistema operativo, y sólo continuaba sus acciones si era Windows 98. A los creadores de 29A también les gustaba jugar con los laboratorios y los medios de comunicación, y en este caso les siguieron el juego (de forma premeditada o no). La CNN dijo de él "Un virus se adelanta a la salida del sistema operativo". Eso fue el detonante de una explosión de noticias en periódicos. Crearon "Marburg", el primer virus polimórfico de 32 bits, propagado por el mundo a gran velocidad, protagonizando diversos incidentes. Las revistas PcGamer y Pc Power Play contenían varios programas infectados en los discos que las acompañaban. El CDROM del juego MGM/Wargames salía al mercado infectado. Llenaba el escritorio de iconos de error critico de Windows, un circulo rojo con un aspa blanca. MrSandman escribió Esperanto, el primero capaz de ejecutarse tanto en Windows como en MacOS. GriYo, MrSandman, y VirusBuster, era los miembros más activos. Precisamente VirusBuster es el que pone punto y final al grupo, al considerarse último miembro activo y no poder contactar con el resto. Desde 1998, Bernardo Quintero los conocía bien, por analizar sus creaciones desde hacía más de una década. De una de las entrevistas exclusivas que Antonio Ropero publicó en PCActual en 1998, se puede extraer:

¿Cuál es el futuro de los virus?
Las nuevas plataformas son cada día más potentes, pero a la vez más complejas. Desarrollar virus será cada vez una labor más complicada, y requerirá más tiempo y más recursos. Los virus, tal y como ahora los conocemos, desaparecerán, para dar lugar a sofisticados hackers electrónicos desarrollados al amparo de instituciones gubernamentales. Toma ya! ;)

Proyectos actuales y metas a medio plazo.
Pronto tendré acabado un virus nuevo, me gusta llamarlo "virus de nueva generación", puesto que aplica conceptos nuevos que pronto serán muy comunes. Te puedo avanzar que Internet es tan importante para este virus como los ficheros .EXE lo han sido para los virus tradicionales.

_ F-Secure opina que en el futuro, además de las localizaciones habituales donde se origina el malware actual, **África y Centroamérica representarán una nueva fuente de crimen informático organizado**.

Se presenta la **AMTSO** (Anti-Malware Testing Standards Organization). Es una iniciativa de la industria antivirus para estandarizar comparativas. Aunque su primera reunión informal tuvo lugar en Reykjavik (Islandia) en mayo de 2007, se decide organizar una reunión formal para dar cuerpo a esta iniciativa en enero de 2008. Más de 40 miembros de distintos países implicados en el tema (casas antivirus, testeadores profesionales de antivirus y otras figuras de esta industria tecnológica) conforman las bases de esta organización cuyo fin es el de crear una serie de guías y herramientas que ayuden a mejorar la calidad y la objetividad de las comparativas que se realizan hoy en día.

Además de Hispasec, la AMTSO incluye a representantes de ALWIL Software, AV-Comparatives, AV-Test.org, AVG Technologies, Avira GmbH, Bit9, BitDefender, Dr. Web, Ltd., ESET, F-Secure Corporation, G DATA Software, International Business Machines Corporation, Kaspersky Lab, McAfee, Inc., Microsoft Corp., Norman ASA, Panda Security, PC Tools, Sana Security, Secure Computing, Sophos Plc, Symantec Corporation, Trend Micro Incorporated y Virusbuster Ltd.

_ La versión 2.0.0.12 de Firefox corrige (entre otras) **una vulnerabilidad descubierta por Gynvael Coldwind (Michael), de Hispasec.** La Fundación Mozilla publica la actualización 2.0.0.12 para sus productos, solucionando más de 10 problemas de seguridad. Una de las vulnerabilidades que permite obtener información sensible del usuario es descubierta por el equipo técnico de Hispasec Sistemas. Se publica un detallado estudio posteriormente, cuando por fin otros navegadores que se veían afectados (todos menos Internet Explorer) solucionan el problema.

_ La primavera se adelanta en Hispasec y **creamos unas nuevas camisetas exclusivas** con las que se premia a los ganadores de un pequeño concurso de critografía que ponemos en marcha.





_ Se popularizan los archivos PDF que aprovechan **vulnerabilidades en Adobe Reader** para infectar sistemas. Adobe publica una alerta de seguridad en su lector PDF. Uno de estos fallos está siendo aprovechado para instalar malware, en concreto Zonebac. El usuario quedaría infectado con sólo abrir un archivo PDF con Adobe Acrobat anterior a la versión 8.1.2. Zonebac es un malware especializado en adware y el payload del ataque se descarga, como viene siendo habitual, de un servidor remoto (no va incluido en el PDF que está siendo distribuido).

_ Aparece una **grave vulnerabilidad en el kernel de Linux** anterior al 2.6.22.17 que permite elevar privilegios a root. Se hace público un exploit. Son decenas de distribuciones las que se ven afectadas. El goteo de parches de distintas casas es continuo.

_ Se descubren nuevos métodos para intentar **eludir los filtros antispam**. Uno de ellos es valerse de los mensajes automáticos de "fuera de la oficina" que utilizan algunos servicios de webmail legítimos. Los spammers se dan de alta en una cuenta de correo (gratuita) que ofrezca la funcionalidad de "auto-responder". En esta notificación se suele añadir hasta qué fecha se estará fuera, teléfonos de contacto adicionales... etc. Son muy usados precisamente en las oficinas para indicar las vacaciones o periodos en los que no se revisará el correo. Cada correo enviado a esa cuenta con la funcionalidad activada, generará un correo de vuelta a quien lo envió con información en principio útil. Lo que hacen los spammers es configurar la respuesta de "fuera de la oficina" con el contenido basura y bombardear esa misma cuenta con emails con el campo 'desde' (from) falseado con listas de víctimas de spam. Otro método de moda en ese momento implica el uso de Google Calendar, por ejemplo.

_ **Cisco** anuncia importantes cambios en la planificación de sus alertas. Decide publicar sus parches de seguridad cada seis meses, en el cuarto miércoles de marzo y el cuarto miércoles de septiembre. Se une así a la política de alertas de seguridad programada de Microsoft y Oracle, entre otros. Las alertas así programadas sólo afectan a su sistema operativo IOS.

_ **Apple Mac OS X** comienza el año publicando un mega parche que soluciona 90 fallos de seguridad. El número de vulnerabilidades aumenta en cada superparche publicado y su gestión de la seguridad lleva meses cuestionada. Más tarde ese mismo año lo demostraría al ser el último gran fabricante en dar solución al gravísimo problema con los DNS descubierto por Kaminsky.

_ En mayo, durante el congreso de seguridad **Confidence 2008** en Cracovia, el equipo de Hispasec alcanza "The Perfect Score" en el reto planteado, salvando todas las dificultades técnicas. En momentos de asueto, Emiliano, Michael y Marcin se codean con Joana Rutowska. Julio se conforma con hacer la fotografía.



_ Microsoft publica una alerta oficial sin parche. Se observa un repunte en los ataques que aprovechan vulnerabilidades en el **Jet Database Engine de Microsoft**, que procesa archivos MDB de bases de datos. Esta librería (en concreto msjet40.dll) sufre desde hace años varios problemas de seguridad que permiten la ejecución de código. Los atacantes envían estos ficheros por correo y, al ser una extensión "habitual" e inofensiva para muchos usuarios, el atacante consigue su objetivo. No se descubre una nueva vulnerabilidad, sino una ingeniosa forma de aprovechar fallos relativamente antiguos. Hasta ahora, las dos vulnerabilidades más graves encontradas en esta librería se hicieron públicas a mediados de 2005 y finales de 2007 y, aunque los fallos son activamente aprovechados por atacantes, no han sido corregidos. Microsoft considera públicamente que los ficheros MDB son "cuasi" ejecutables, inherentemente inseguros, y que el hecho de que se pueda ejecutar código a través de ellos no debe escandalizar más que el hecho de que alguien haga doble click sobre un .exe y espere que algo sea ejecutado en el sistema. Pero se descubre que, ingeniosamente, ahora se consigue que sea explotable a través de archivos .DOC y no directamente

desde los MDB, (que Microsoft bloquea en sus clientes de correo). La 'excusa' de que los MDB son inseguros y por ello no es necesario parchear la librería, deja de ser válida. La librería sería parcheada y distribuida poco después.

_ Una **central nuclear en Georgia** debe realizar un apagado de emergencia durante 48 horas tras la instalación de una actualización de seguridad que desestabiliza un ordenador, perteneciente a la red de control de la planta.



_ En junio Eva Chen, cofundadora y CEO de Trend Micro, declara **"la industria antivirus apesta"**. Los atacantes van por delante y la industria se ha quedado atrás. Está harta de invertir y no obtener los resultados esperados. Los niveles de infección son cada vez mayores y no hay visos de mejora a no ser que se modifique radicalmente la filosofía que hasta ahora han venido arrastrando los antivirus.

_ La versión **2.0.0.14 del navegador Firefox** corrige una sola vulnerabilidad, algo nada habitual teniendo en cuenta que cada nueva versión soluciona normalmente entre 4 y 8 vulnerabilidades. El problema de seguridad que corrige, además, tiene su origen en una actualización anterior. La versión 2.0.0.13 corregía una sola vulnerabilidad descrita como una denegación de servicio a través del recolector de basura de JavaScript. El problema es que se sabe que bajo ciertas circunstancias, "cuelgues" de esta misma naturaleza han podido llegar a ser explotables en el pasado, y por tanto, permitir la ejecución de código. Para estas fechas, Firefox tiene casi entre un 16 y un 20% de mercado. Internet Explorer entre un 73 y un 78%, Safari entre un 3 y un 6% y Opera un 0.80%.

_ Hispasec participa en un taller de trabajo de un proyecto europeo llamado **FORWARD**. Básicamente se trata de una iniciativa de la Unión Europea que intenta crear un grupo de expertos en materia de seguridad informática que ayude no solo a ver con perspectiva lo que ocurre en estos momentos en el mundo, sino que también se aporten ideas sobre cuáles se sospecha serán las futuras amenazas a largo plazo. El primer workshop se celebra en Gottebörg, Suecia. Está organizado por la Universidad Tecnológica de Chalmers, uniendo la experiencia de empresas, universidades y entidades como la propia Comisión de la Unión Europea que se encarga de estudiar estos asuntos. Entre los participantes se encuentran: Banco de Austria, Boeing, British Telecom, Cisco, Combitech, Deep Blue, EADS, ENISA, FORTH, France Telecom, Fraunhofer, G-Data, Hispasec , Hitachi, Instituto Eurecom, Instituto Waterford de Tecnología, Instituto de Ciencias de la Computación (Grecia), Ipp-BAS, Joint Research Centre of the UC, Nokia, Packet General Networks, Panda Security, Parque Científico de Lindholmen, SEMA, SINTEF, Symantec, S21 Sec, Telekom Austria, TeliaSonera, TU Darmstadt, Universidad de Mannheim, Universidad de Ulm, Universidad de Vrije, Universidad Northeast, Universidad de Columbia, Universidad Carnegie Mellon, Universidad Técnica de Viena, Università degli Studi di Milano, Universidad Tecnológica de Chalmers, Virgin Charter, Volvo, Universidad de Koc y UCSB (USA).



_ Symantec, curioseando en los archivos de ayuda del paquete de **malware Zeus**, descubre un curioso "acuerdo". Zeus crea una botnet con una interfaz muy cómoda con la que manejar a los zombis. En su acuerdo de licencia, aparte de la prohibición expresa de distribución descontrolada, aplicar ingeniería

inversa y demás condiciones que se aplican en las licencias "habituales" de software, se puede leer (en ruso): "En caso de que se detecte la violación de los acuerdos, el cliente pierde el soporte técnico. Además, el código binario de la botnet será enviado inmediatamente a las casas antivirus."

_ Según G Data, **España ocupa el noveno puesto mundial en número de sistemas zombi**, casi en empate técnico con Estados Unidos y Rusia. Lo que además indica que somos grandes productores de spam, una de las funciones más importantes de los sistemas secuestrados. El informe está realizado por G Data según la geolocalización de las direcciones IP. El número de zombis utilizados cada día ronda una media de 350.000, con momentos en los que se utilizan hasta 700.000 ordenadores para los distintos fines de estas botnets. De los diez países más infectados, la mayoría pertenecen a Europa. Según el informe, es el continente que goza de líneas de conexión más rápidas y mayor número de ordenadores.

_ Microsoft lanza el **Service Pack 3** para el sistema operativo más popular de la compañía. Tras un pequeño retraso por cierta incompatibilidad con su Dynamics RMS, se ofrece para descarga directa.

_ El plugin del idioma vietnamita para Firefox 2 es distribuido desde el sitio oficial (y durante semanas) **infectado con adware**. Window Snyder, responsable de seguridad de Mozilla, declara "todo el que haya descargado una copia del paquete de idioma vietnamita desde el 18 de febrero, está infectado". Esto motivaría un mayor control sobre los repositorios de plugins de la fundación.

_ En julio Bernardo Quintero es nombrado **MVP de seguridad** (Most Valuable Proffesional). El promotor de la nominación es Chema Alonso (MVP de Seguridad en Microsoft, de Informática64), el otro (y tercero hasta la fecha) MVP de seguridad en España. A pesar de que Bernardo ha sido muy crítico con la seguridad de Microsoft, el galardón es otorgado por su extraordinaria independencia, nivel técnico y objetividad.

Es el año del descubrimiento de grandes fallos catastróficos. La **criptografía en Debian sufre un grave revés**. Se descubre que el generador de números aleatorios del paquete OpenSSL de Debian es predecible. Esto hace que las claves generadas con él ya no sean realmente fiables o verdaderamente seguras. El problema tiene (y tendrá por muchos años) una importante repercusión y numerosos efectos colaterales en otros paquetes y distribuciones. Luciano Bello, desarrollador de Debian, daba la voz de alarma. Sólo afecta al OpenSSL de Debian porque esta distribución parchea su propia versión de OpenSSL, a su manera. En este caso, elimina una línea crucial de código que limita al generador a producir sólo 2^18 claves (solamente 262.144), en vez de poder elegir claves de, por ejemplo 2^1.024 posibilidades. La noticia capta la atención de los medios. No sólo Debian se ve afectada, sino cualquier distribución que use certificados y claves generadas con el paquete vulnerable desde 2006. Afecta a las comunicaciones SSH que se autentican con claves asimétricas e incluso certificados SSL alojados en páginas web. Con el tiempo se sabría que el fallo sería aprovechado por atacantes para acceder a sistemas legítimos.

_ Después de algo más de un año de trabajo entre bambalinas, y bajo el amparo de la Unión Europea, comienza su andadura el proyecto **WOMBAT (Worldwide Observatory of Malicious Behaviors and Attack Threats)**, formado por un grupo de universidades y empresas internacionales, entre las que se encuentra Hispasec.

Básicamente, WOMBAT pretende recolectar grandes cantidades de información sobre elementos

maliciosos que puedan afectar tanto a empresas como a usuarios. Realizado en tiempo real, no se pretende solamente tener una visión más real de lo que realmente sucede en Internet, sino modelar estos comportamientos en la medida de lo posible. En la lista de participantes en este proyecto se cuenta con la participación de varias universidades. La Universidad Técnica de Viena y la gente que desarrolló Anubis, también la Universidad de Vrije (Ámsterdam), que entre otras cosas aportará su experiencia en diversos tipos de honeypots. La Politécnica de Milán aportará también su conocimiento en estas lides, que incluye aspectos tan interesantes como las tecnologías IDS. Por parte de los CERT, se cuenta con la experiencia de NASK (Polonia), y también con la perspectiva de los ISPs gracias a la colaboración del departamento de I+D de France Telecom (Orange). Desde Hispasec colaboraremos con nuestra experiencia en el mundo del malware, y con la perspectiva que nos da mantener en funcionamiento **VirusTotal**.

_ Se detecta una ola de troyanos bancarios que tienen como objetivo **a los clientes de ING Direct España (ingdirect.es)**. Los troyanos capturan todos los datos necesarios para suplantar la identidad de los usuarios legítimos, incluyendo la tarjeta de coordenadas para poder realizar transferencias desde sus cuentas.

_ Se lanza **Firefox 3** con gran éxito (animado por una campaña que pretende romper el récord de descarga durante las primeras 24 horas de disponibilidad). Zero Day Initiative (ZDI) publica el descubrimiento de un agujero de seguridad tan solo 5 horas después (aunque es bastante más que probable que tuvieran conocimiento del fallo desde la aparición de las primeras betas, pero hubiesen esperado al lanzamiento oficial para hacerlo público). Los investigadores de ZDI confirman que la vulnerabilidad podría permitir la ejecución de código arbitrario de forma remota con los permisos del usuario ejecutando la aplicación, aunque el fallo no parece estar siendo explotado.

Desde el 8 de julio se produce uno de los episodios más curiosos vividos nunca en la Red. Se publica ese día una **actualización masiva para la mayoría de los dispositivos en Internet que utilizan DNS**. Se dice que había sido descubierta una vulnerabilidad que permitía falsificar las respuestas DNS y, por tanto, redireccionar el tráfico. Casi todos los grandes y pequeños fabricantes y programadores actualizan sus sistemas y se intentan mantener los detalles técnicos de la vulnerabilidad ocultos, por la gravedad y el potencial impacto que podría suponer. Cisco, Microsoft, BIND... todos publican una nueva versión o actualizan sus sistemas para solucionar un misterioso fallo. Con la mínima información disponible, y un poco de ingeniería inversa, las especulaciones comienzan a volcarse en Internet. Se sabe que los parches añaden aleatoriedad al cálculo de puertos e identificadores. Este es un problema endémico del protocolo DNS y desde hace mucho se sabe que no es la mejor solución para asegurarlo. Es por esto que se apuesta desde un principio por que la vulnerabilidad de Kaminsky se trata en realidad de una nueva forma más eficaz de engañar a los servidores DNS para que den respuestas falsas, gracias a un fallo inherente del protocolo (y así se confirmaría). Dan Kaminsky es el responsable de orquestar la macro actualización y el que encuentra el gravísimo fallo. Afirma que dará los detalles técnicos durante la conferencia Black Hat en agosto. Pero se le adelantan. Thomas Dullien, el CEO de la compañía Zynamics (también conocido como Halvar Flake), se aventura semanas después a publicar en su blog su particular visión de lo que podía ser el problema descubierto por Kaminsky, sin tener conocimiento previo de los detalles. Y no se equivoca en su teoría. Por si fuera poco, sería accidentalmente confirmado desde el blog de una empresa que conocía a fondo la vulnerabilidad. Finalmente los detalles se harían públicos, demostrando que mantener un grave problema en secreto hasta que exista parche, es factible siempre

que no se diga que existe. Esto haría que se replanteara lo débil de algunos protocolos que sustentan la red y que fueron diseñados en otros tiempos.

_ A finales de julio se crea un gran revuelo con la aparición de un nuevo troyano que afecta a archivos multimedia. Este malware, que muchas casas antivirus denominan **GetCodec**, emplea una técnica de infección que no había sido vista hasta el momento. Hispasec publica un amplio estudio técnico al respecto. Se propaga encubierto como cracks en páginas de warez y cracks. Es totalmente silencioso, lo que induce a pensar que tan sólo se trata de otro crack corrupto más. Tras su ejecución, el troyano busca todos aquellos archivos con extensiones .MP2 .MP3 .WMA .WMV .ASF. El formato ASF es un formato propietario de Microsoft empleado por Windows Media Player que permite introducir secuencias ejecutables en flujos de audio/video. El troyano aprovecha esta propiedad para introducir en los archivos multimedia de la víctima una secuencia que solicita la descarga de un codec falso desde un Sitio Web. Este codec es a su vez otro troyano, aunque la técnica podría emplearse para servir cualquier tipo de contenido. Este método de infección también funciona con los archivos MPx porque el troyano los convierte primero a formato ASF para después inyectarles el código malicioso. De forma que un archivo con extensión .MP3 puede estar infectado. El espécimen modifica la configuración del usuario de tal forma que este nunca llega a notar que sus archivos multimedia han cambiado, sin embargo, todo aquel que no esté infectado e intente reproducirlos sí notará el cambio. Cuando se reproduce un archivo multimedia infectado, en una máquina limpia, Windows Media Player despliega una ventana solicitando la descarga de un codec falso. Este codec puede ser cualquier otro tipo de malware. Al aceptar la descarga se produce la infección. Hispasec crea una herramienta específica para eliminar este troyano.

_ **"Como impresionar a las chicas traspasando la protección de memoria con el navegador"**. Con ese jocoso título, los investigadores, Alexander Sotirov y Mark Dowd, muestran a una expectante audiencia en las conferencias Black Hat 2008 cómo traspasar las protecciones de memoria de Windows Vista y ejecutar a través del navegador cualquier tipo de código. Consiguen burlar el ASLR y el DEP bajo ciertas circunstancias. Estas son dos de las soluciones introducidas y potenciadas en Microsoft Vista con respecto a la seguridad. Los investigadores se saltan estas barreras.



_ A principios de septiembre Google lanza (después de muchos rumores) casi por sorpresa (como suele hacer con todo) **su nuevo navegador, conocido como Chrome**. Una semana después, Internet se inunda de comentarios sobre todos los aspectos de esta nueva aplicación y en particular sobre su seguridad. Muchos comentarios, exploits, actualizaciones y aclaraciones después, el gobierno alemán desaconseja explícitamente el uso de este navegador, más por la acaparación de datos personales que puede llegar a realizar Google que por el problema que el navegador en cuestión de seguridad puede suponer. Algunas de las vulnerabilidades encontradas son serias, la mayoría sin embargo, simples denegaciones de servicio. El navegador se hace muy popular durante algunas horas, alcanzando cotas de uso de hasta el 7%. Pero rápidamente la moda pasa y pocos vuelven a usarlo tras una primera impresión. En realidad el navegador, aunque innovador en algunos aspectos, carece absolutamente de funcionalidades prácticas e imprescindibles con las que ya cuentan sus competidores. Google debe además modificar su EULA (End User License Agreement) inicial por resultar sorprendentemente abusiva con los datos personales.

_ El 10 de septiembre, el Daily Telegraph alerta de que un grupo de atacantes griegos ha desfigurado una de las páginas relacionadas con el **famoso LHC (Large Hadron Collider)**. El experimento cuenta obviamente con una inmensa red de sistemas conectados. Una de las páginas públicas (www.cmsmon.cern.ch), forma parte del CMSMON, que controla el software que utilizan los científicos para analizar los resultados de las colisiones. La idea era usar esta página para que todo el mundo pudiese disfrutar en

directo de los resultados obtenidos.Aparece desfigurada y con un mensaje escrito probablemente por un grupo de atacantes de poca monta. Calificaban de niñatos a los responsables de seguridad de la red, que en última instancia es el CERN (European Organization for Nuclear Research). En la página se ofrecen ciertas evidencias de que quizás podrían haber llegado un poco más lejos de la simple desfiguración de la página. Una de las declaraciones del portavoz del CERN, James Gillies, aparecidas en la nota original del Daily Telegraph es que: "Tenemos diferentes niveles de red, una red de acceso general y una mucho más restringida para las cosas sensibles que hacen funcionar el LHC" pero esta afirmación lógica es omitida en otros medios en favor del sensacionalismo. No se sabe bien cómo, es bastante más que posible que hayan podido entrar en la zona de acceso general, los vectores de ataque son muchos. Sin embargo, ese salto a la red verdaderamente sensible, por mucho que fanfarroneen los atacantes, habría sido mucho más complejo.

_ Un atacante accede al **correo personal de Sarah Palin**, la candidata a vicepresidenta en Estados Unidos con el republicano John McCain. Se da a conocer su email personal, alojado en el servicio de correo público de Yahoo! y usado además para cuestiones gubernamentales. A un tal "Rubico" le cuesta apenas una hora cambiar la contraseña del correo de Sarah. Se hacen públicas conversaciones y fotografías personales. El método es calificado por las agencias de noticias como "un magistral ataque cirbenético". La verdad es que simplemente se usa el servicio de recuperación de contraseña, la Wikipedia y Google para acertar la pregunta secreta y poder acceder a los emails. Esto ya le ocurrió a Paris Hilton en febrero de 2005.

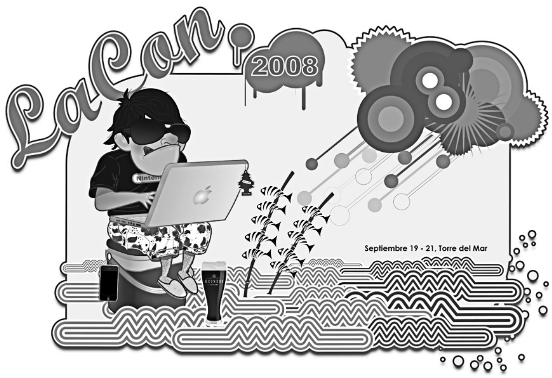
_ En agosto, durante la Black Hat, se habla de nuevo de **la mayor vulnerabilidad de Internet** al demostrar dos investigadores una nueva técnica que permite interceptar el tráfico de Internet a una escala global. Tony Kapela y Alex Pilosov demuestran por fin de forma empírica un problema que se presuponía teórico hasta ahora. Cualquiera con un router BGP podría desviar el tráfico de cualquier gran nodo y devolverlo de forma transparente. Se trata de nuevo de un fallo de diseño en el protocolo BGP (Border Gateway Protocol) que permitiría interceptar e incluso modificar todo el tráfico de Internet no cifrado. BGP es un protocolo que se utiliza para intercambiar tablas de enrutamiento entre sistemas autónomos (AS). El problema es que nunca se ha llegado a idear un sistema que realmente autentique a ambas partes, y los routers estén así seguros de que la información recibida desde un AS es legítima y viene del sitio adecuado.

_ Se detecta en Europa un tímido intento de **revivir los virus de macro**, a través de un documento en Microsoft Word que está siendo enviado a través de spam. El virus no representa ninguna evolución del concepto y no se le espera repercusión alguna, pero supone un renovado y discreto interés por este tipo de malware, prácticamente extinto desde finales de los 90.

_ Por tercera vez en el año, se habla de **la mayor vulnerabilidad encontrada en la Red**. La compañía sueca Outpost24 dice que descubrió en el 2005 (aunque lo saca a la luz 3 años después, posiblemente animada por los acontecimientos vividos este año con el DNS) varias **vulnerabilidades de base en el mismísimo protocolo TCP/IP** que podrían permitir la caída de cualquier aparato con comunicación en la Red. Es la llamada "denegación de servicio de bajo ancho de banda". Aunque no se conocen los detalles, todo son conjeturas. Se puede tratar de una nueva forma de aprovechar una vieja debilidad conocida del TCP/IP. La denegación de servicio puede ser de muchos tipos. Lo normal es que permanezcan caídos mientras dure el ataque (como ocurre con un DDoS, por ejemplo), pero se han dado casos en que se agotan sus recursos y se necesita un reinicio con una mínima cantidad de tráfico. Por si fuera poco dicen no conocer una implementación de la pila que no sea vulnerable. Se reabre con fuerza el debate sobre el uso de protocolos diseñados hace décadas en la Internet de hoy.

_ Las **redes sociales** están de moda. Por ello, FaceBook y Myspace se convierten involuntariamente en grandes distribuidoras de malware. Los atacantes crean cuentas falsas donde alojan vídeos y enlaces a malware, que envían a las víctimas como si se tratasen de amigos que quieren contactar con ellos.

_ En septiembre, junto al grupo 48bits.com, Hispasec organiza por primera vez **LaCon**, una serie de conferencias para un grupo muy reducido de asistentes que alcanzan un altísimo nivel técnico. Durante las dos jornadas, ponentes expertos de toda España desvelan inconfesables secretos de seguridad, vulnerabilidades, ingeniería reversa sobre móviles, herramientas... por las mañanas y las noches, aprovechan para conocer las playas y los bares malagueños.



_ A mediados de 2008, la configuración estándar de un sistema puede ser:

Microprocesador Intel Core 2 Duo con 3 MB de caché L2 por core, 1.333 Mhz FSB (Front Side Bus), y con soporte hardware para virtualizacion.

2 GB de RAM DDR2; Disco duro de 320 GB; Tarjeta de sonido y red integrada en placa madre; Tarjeta gráfica Ati Radeon HD3850; Lector multi-tarjetas; Regrabadora de DVD; Monitor TFT de 19”

Y pagar 400 euros por ella. Por menos de 200 euros más, se podría tener un Quad (cuatro núcleos). Por unos 30 euros más, 4 GB de RAM, por 60 euros más 500 GB de disco duro. Una grabadora de Blue Ray encarece en 150 euros el sistema. Si se quiere equipar al ordenador con un disco duro externo de 750 GB, podría costar 100 euros. Un monitor de 21 pulgadas solo cuesta 30 euros más. También se pueden comprar sistemas de gama baja, sin monitor, por 250 euros.

Esta misma configuración en un portátil, llega a los 700 euros. Una cámara fotográfica digital de 5 megapíxeles y con una tarjeta de 2 GB de memoria, que permite grabación ilimitada de vídeo, cuesta menos de 100 euros.

_ En octubre, **Sun Microsystem**, creador del Java Runtime Environment (JRE) promete que por fin **eliminará las versiones antiguas del JRE que quedan en el sistema** cuando se actualiza. En JRE6 Update 10 se incluye una funcionalidad (patch-in-place) que hace que se elimine a sí misma (pero no al resto anterior versiones de JRE que puedan estar instaladas en el sistema) cuando aparece el Update 11.

_ El 5 de noviembre Adobe publica (entre otros boletines de seguridad para otros productos) una **actualización para Adobe y Adobe Reader 8 que soluciona varias vulnerabilidades** que permitían la ejecución de código. Uno de los fallos más graves se da en la función JavaScript “util.printf”, provocado por un error al procesar cadenas de formato. Adobe es advertida del problema en abril de 2008. Foxit Reader, otro popular lector de PDF, también sufre una vulnerabilidad muy parecida. Foxit lo soluciona un mes después, en abril, mientras que Adobe publica a principios de noviembre el parche. Poco después aparece información pública con los datos técnicos de la vulnerabilidad y **comienza a ser aprovechada por atacantes para instalar malware**.

_ Los investigadores alemanes Erik Tews y Martin Beck dicen haber conseguido **saltarse parcialmente la seguridad que proporciona WPA** (Wi-Fi Protected Access) en las redes inalámbricas. WPA sustituye al inseguro WEP (Wired Equivalent Privacy), que fue vencido pocos años después de su estandarización y que hoy en día es un cifrado obsoleto. Este descubrimiento induce a muchos a usar por fin el WPA2 (WPA con AES, en vez de con TKIP). El método descubierto no permite recuperar la contraseña y tampoco influye el método de autenticación. El problema está en el cifrado. Aunque el ataque está limitado a descifrar paquetes concretos o inyectar nuevos (y sólo una pequeña cantidad), sirve como alarma para migrar al otro estándar más seguro.

El ataque sólo funciona si se utiliza el cifrado TKIP, no el AES y requiere de unos 15 minutos para poder inyectar algún paquete ARP. Un año después se publicaría otro estudio basado en este ataque en el que se explica que este tiempo se podría reducir a un minuto.

_ Microsoft introduce en sus boletines un nuevo valor llamado **índice de explotabilidad** (exploitability index) que indica las posibilidades de que se cree un exploit para cada vulnerabilidad. Además, continúa activando el mayor número de killbits posibles para evitar ataques a través de ActiveX vulnerables.

_ **La Fundación Mozilla** advierte que la rama 2 de Firefox acababa con la versión 2.0.0.19. Esta sería la última en la que se solventarían vulnerabilidades. Sin embargo en diciembre **se ve obligada a lanzar urgentemente la versión 2.0.0.20** que corrige uno de los fallos que se suponían solucionados en la 2.0.0.19 para Windows. Al parecer, durante el proceso de empaquetamiento y firma de la versión para Windows, olvidaron incluir una de las correcciones.

_ Nuestro compañero Michael disputa y **gana la final del Security Days** en su sexta edición, repitiendo el mismo resultado que el año anterior.

_ La revista **Re@ Seguridad**, nos otorga en los Trofeos de la Seguridad TIC 2008, el **"Trofeo extaordinario del Jurado"**, sin ni siquiera habernos presentado a esta candidatura. Según se puede leer en la nota de prensa: "Tras un moderado debate sobre las propuestas que este año han puesto sobre la mesa los miembros del CTA, para distinguir a la persona, entidad o colectivo del sector de la seguridad TIC por sus valores humanos, acciones meritorias o labor extraordinaria en pro del desarrollo y difusión de la cultura de la Seguridad TIC, el jurado decidió homenajear con el "Trofeo Extraordinario del Jurado" a la empresa española Hispasec Sistemas. La mención a esta firma, que comenzó su actividad profesional en 1998, se debe a su carácter de servicio público y gratuito para la comunidad y su propósito de divulgar y concienciar a los usuarios de la importancia de la seguridad en las TI; por su carácter pionero y su extensión a Latinoamérica."

_ Un día antes del segundo martes del mes de diciembre un mensaje en un foro chino hace pública **una vulnerabilidad en Internet Explorer 7** para la que no existe parche oficial, no necesita interacción por parte del usuario y permite, si consigue explotar el fallo, ejecutar código arbitrario con los permisos del usuario. Microsoft lo soluciona con **un boletín fuera de su ciclo habitual** diez días después.

17/01/2008 Un año de Storm Worm

El 19 de enero de 2008 se cumple un año del primer ‘avistamiento’ de Storm Worm. Hoy en día es una de las epidemias más extendidas, y cumple un año con un índice aceptable de infección que sin duda le permitirá permanecer aferrado a los primeros puestos durante bastante semanas más. Muchos lo llaman Storm, otros Peacomm o Nuwar. Es difícil seguirle el juego. Se dice que el primer Storm Worm fue visto por primera vez en Helsinki el 19 de enero de 2007. Desde entonces, se ha posicionado como una insistente epidemia de nuestro tiempo y siempre ha resultado bastante mediático.

Storm Worm comenzó como un ejemplo de libro en cuestión de métodos de infección. Un archivo ejecutable adjunto a un correo que prometía un vídeo sobre las tormentas que sufría Europa en aquel momento. Sin embargo, una vez conseguida una base sustancial de víctimas e infectados, estos mismos sistemas troyanizados comenzaron una campaña de expansión a través de spam que todavía inunda las casillas de correos.

Luego ha mejorado con distintas campañas. Cada cierto tiempo, cambia el método de infección. Desde el adjunto hasta la invitación a visitar páginas web que no solo pretendía que la víctima descargase el troyano, sino que intentaba aprovechar vulnerabilidades de todos los navegadores para conseguir la ejecución. Otro de los puntos fuertes de este virus ha sido su capacidad de poliformismo en servidor. El archivo que descargaban las víctimas podía mutar hasta varias veces por minuto, detectándose literalmente decenas de pequeñas y grandes variaciones por día alojadas en servidores.

Las campañas con la que Storm ha enviado correos basura para incitar a la infección han sido de lo más variopintas... desde invitaciones a la descarga de juegos, pasando por premios de la lotería, cirugía barata, contraseñas para portales especiales... y, la última, invitaciones de amor para el día de San Valentín.

Hace tiempo que no se recordaba una epidemia tan duradera. Si bien no se percibe igual que en los tiempos del Klez (un año en el “top ten” una proeza para ser el año 2003), Code Red, Nimda, MyDoom.... Solo NetSky, en especial su variante NetSky.P, puede decirse que vaya a la zaga. Descubierto en marzo de 2004, no es raro encontrar sistemas infectados con esta variante todavía.

Y no es solo que Storm Worm mute con nuevas versiones, sino que se ha convertido en un complejo sistema multi-modular que se sirve de cientos de servidores comprometidos o no, una capacidad de mutación endiablada, y una modularidad que permite que sus funcionalidades cambien continua y radicalmente. Por tanto Storm Worm no se podría clasificar como un troyano sino como un complejo sistema perfectamente orquestado, cambiante y eficaz. Muy al estilo malware 2.0.

Existen otras familias, como los Sinowal o Zlob, que de forma mucho más silenciosa, llevan también presentes en Internet desde hace muchos meses, aunque no de manera tan notoria. De hecho, el ratio de detección en VirusTotal de este tipo de familia (Sinowal) suele ser del 25%.

Sergio de los Santos

01/04/2008 Mitos y leyendas: Las contraseñas en Windows I (Tipos de ataques)

Vamos a escribir algunos textos más o menos técnicos sobre las contraseñas en Windows. Existen diferentes mitos y leyendas que pensamos no han sido explicados de forma directa (y sin aspavientos) en la mayoría de la literatura que hemos leído al respecto. Publicaremos de sencilla, una serie de artículos aclarando detalles que consideramos interesantes sobre las contraseñas locales en Windows, sus puntos fuertes y débiles.

Cuando nos presentamos en una máquina Windows, la contraseña que proporcionamos debe estar almacenada en algún lugar para que el sistema operativo la reconozca y bien nos deje pasar, bien rechace el acceso. Almacenar la contraseña y compararla sin más con la que proporciona el usuario, sería una muy mala política de seguridad. Cualquiera con acceso al disco duro podría robar la contraseña en texto plano. Lo que se almacena en realidad es el resultado de aplicar un algoritmo a la clave introducida. Esto da como resultado una "firma" (o tradicionalmente llamado "hash"), un valor que en teoría sólo es producido por una contraseña en concreto. Son firmas lo que siempre se comparará entre sí, nunca contraseñas. En Windows, ese hash se encuentra físicamente en el archivo de nombre SAM (Security Account Manager) para contraseñas locales y en el archivo ntds.dit del controlador de dominio para los usuarios que se validan contra controladores de dominio. Nos centraremos en las contraseñas locales.

Para calcular los hashes que se almacenan en la SAM, Windows XP y anteriores utilizan por defecto dos algoritmos para cifrar cada clave: LM (por compatibilidad hacia atrás) y NTLM, más avanzado y estándar. Vista usa (por fin) sólo NTLM y no calcula ni almacena el inseguro LM por defecto. Un atacante necesitaría tener acceso a estos hashes (uno, otro, o los dos) para intentar calcular a partir de ellos las contraseñas en texto claro (aplicándoles fuerza bruta, o métodos más sofisticados como las tablas rainbow).
Windows no añade 'sal' a las contraseñas

Uno de los problemas históricos del almacenamiento de claves en Windows es que no 'saltea' las contraseñas. No añade, como UNIX por ejemplo, un trozo aleatorio de caracteres a la hora de calcular el hash. Con esto se evitaría que una misma contraseña de dos usuarios distintos, produjese una misma firma. Esto supone un problema de seguridad, porque si un atacante de Windows tiene acceso a estos hashes y dos son iguales, puede tener la certeza de que esos dos usuarios tienen la misma contraseña, incluso si no sabe cuál.

Tipos de ataque

Existen básicamente dos métodos con los que obtener estos hashes. Uno es "offline" y tiene como barrera (evitable) una funcionalidad de Windows de la que hablaremos en el futuro. Otra es "online" y muestra los hashes tal cual.

Volcado de los hashes "online"

Una forma de obtener los hashes de las contraseñas es conectarse al proceso LSASS (Local Security Authority Subsystem) como administrador (o alguien con permisos equivalentes) y volcarlos. LSASS es el proceso que autoriza y maneja todo el tinglado de las contraseñas introducidas en Windows. Mantiene una copia en memoria de estas firmas contra las que compara y valida para ofrecer el token de credenciales correspondiente. Conectarse a este proceso y volcar los hashes "en vivo" en memoria no es complicado gracias a programas como pwdump, que en sus distintas versiones, permite engancharse al proceso y mostrar los hashes de todos los usuarios locales del sistema.

Este método mostrará en claro el hash LM y NTLM con el que Microsoft compara todas las contraseñas

que le introducimos y ahora sí se podrá realizar un sencillo ataque de fuerza bruta contra ellos.

Volcado de los hashes "offline"

Si no se tiene acceso al proceso en memoria, bien porque el sistema esté apagado, bien porque no se disfruten de los permisos necesarios, existen otros métodos. Como hemos dicho al principio, un lugar especialmente delicado en Windows (equivalente al etc/passwd de los sistemas basados en UNIX) se ubica en %systemroot%\system32\config\sam. En todo momento el archivo está manejado y bloqueado por el proceso de sistema por lo que no puede ser movido, copiado o accedido mientras el ordenador esté en marcha, ni siquiera por el administrador.

Esto no impide realmente que alguien pueda hacerse con el archivo. Existen muchas maneras de llegar a ese fichero sin pasar por Windows. Arrancar en un sistema Linux alojado en otra partición, o cualquier otra forma de montar particiones NTFS... (Live Cds, por ejemplo). Otros métodos consisten en buscar otros archivos SAM diseminados por el disco duro. Microsoft guarda una copia de seguridad del archivo en varios directorios, como por ejemplo en %systemroot%\repair cuando el sistema es instalado. En este directorio se encontrará un archivo SAM de menor peso que "el oficial" y con fecha de instalación del sistema. Esta SAM "de repuesto" no se modificará y contendrá la primera contraseña que se le indicó a Windows, aunque el usuario haya modificado la clave de administrador posteriormente. Este archivo no está tomado por ningún proceso, se puede leer por cualquiera, por tanto es necesario vigilar especialmente los permisos NTFS para controlar su acceso.

También puede existir una copia de la SAM en %systemroot%\winnt\system32\config\sam.bak, que tampoco se encuentra bloqueada por ningún proceso. Por último, si el administrador ha realizado copias de seguridad, es posible encontrar comprimido un %systemroot%\windows\repair\sam._ que se puede expandir con el comando de Microsoft "expand".

Una vez que se ha tenido acceso al archivo en cuestión, sea con el método que sea, se puede "volcar" su interior con herramientas como samdump, disponible de forma gratuita desde hace años. En teoría, al volcar este archivo deberíamos obtener los hashes LM y NTLM de las contraseñas. Pero esto no es así. A partir de Windows 2000, Microsoft utiliza por defecto el sistema adicional de cifrado Syskey. Samdump volcará una versión a su vez cifrada de los verdaderos algoritmos de cifrado de Microsoft LM y NTLM. Con Syskey como medida adicional de seguridad sobre el sistema que almacena las contraseñas, Microsoft introdujo una capa más de seguridad, un cifrado de la SAM que dificulta (no demasiado si no se utiliza bien) los ataques "offline" de fuerza bruta o diccionario sobre este archivo. Syskey estaba destinado a evitar estos ataques (pues cifra sobre cifrado) pero en la práctica, ni Syskey ni los cifrados LM/NTLM han aportado realmente seguridad adicional. Se sigue dependiendo de la fortaleza de la contraseña que elija el usuario.

¿Por qué el Syskey no suele aportar realmente seguridad? ¿Cómo funcionan realmente los hashes LM/NTLM? Lo estudiaremos en profundidad en un próximo artículo.

Sergio de los Santos

23/04/2008 ¿PayPal bloqueará a los navegadores "inseguros"?

Se ha escrito mucho sobre esta medida decidida por PayPal, sin duda, un peso pesado en Internet y cuyos

movimientos se siguen con lupa. Como suele ocurrir en estos casos, la noticia ha sido en parte confundida y al parecer la mayoría de los medios no han sabido transmitir realmente la idea de PayPal. Como de costumbre, los medios generalistas han terminado aprovechando para señalar con el dedo a los de siempre, con el mensaje de siempre, y olvidando realmente cuál es el objetivo de la compañía.

PayPal es el sistema de pago líder en Internet. Permite ingresar o recibir dinero en cuentas particulares o ajenas con sólo conocer la dirección de correo de un usuario de PayPal. PayPal es la compañía, junto con eBay, que más ataques phishing sufre cada día. Las contraseñas robadas de usuarios se cuentan por decenas cada hora. Como medida para paliar este problema, la compañía ha anunciado que bloqueará a los 'navegadores inseguros' y aquí parece que comienza la confusión. Es importante destacar que la medida de PayPal está destinada a paliar el phishing, y sus 'navegadores inseguros' se mueven exclusivamente en este contexto del fraude online, y no en ningún otro donde tengan que ver los problemas de seguridad o las vulnerabilidades.

¿Qué es entonces un navegador inseguro para PayPal? La respuesta no tiene nada que ver con vulnerabilidades, problemas de seguridad o nada parecido, aunque muchos han querido llevar la noticia a este campo. Por un lado, PayPal considera inseguros a los navegadores antiguos que han dejado de tener soporte y que no incorporan tecnología antiphishing (desarrollada en los últimos años). Como simple ejemplo, menciona que todavía es visitada por usuarios que utilizan Internet Explorer 4, y que a estos no les permitirá el acceso. Navegar con Internet Explorer 4 o cualquier otro navegador que no recibe soporte ni actualizaciones de seguridad desde hace años es un completo suicido tecnológico para el sistema que lo utilice. Probablemente, que un usuario de IE 4 pique en un phishing de PayPal o no, es el menor de sus problemas.

PayPal utiliza una analogía para explicar lo que pretende: "Dejar que los usuarios de estos navegadores visiten la página de PayPal es como permitir a una factoría de coches que los fabrique sin cinturón de seguridad". Al parecer PayPal avisará durante un tiempo a sus visitantes si detectan estos navegadores, y luego los bloqueará.

¿Qué otro parámetro utiliza PayPal para calificar de inseguro a navegador? Pues que no utilice la tecnología Extended Validation SSL. PayPal ha invertido en estos nuevos certificados SSL (que no son baratos) y obviamente quiere sacarles provecho. Extended Validation SSL es una buena idea. Explicado de forma sencilla, los certificados que cumplan el Extended Validation SSL autentican al servidor (como los certificados tradicionales), pero a efectos prácticos permiten que el navegador que visita la página que tiene estos certificados, muestre de forma mucho más clara que la página es efectivamente la que se quiere visitar. Sería como si el navegador hiciera por nosotros la operación de pulsar sobre el candado cuando nos conectamos por SSL a una página, y verificara la ruta de certificación, el domino válido... todo de forma automática y visual. Si el servidor es seguro, se muestra en la barra de direcciones un color verde. Un usuario puede así de un solo vistazo dar por seguro que el servidor al que se está conectando es el correcto, y que no se está usando un certificado válido, pero falso.

Por ahora, sólo Internet Explorer 7 soporta de serie la correcta interpretación de certificados EV SSL. Firefox 2 necesita un plugin y Opera ha dicho que lo implementará. Safari no se ha pronunciado. Quizás, con el tiempo, PayPal obligue a los usuarios a utilizar un navegador que soporte EV SSL, pero para entonces (dentro de años) probablemente sea algo que todos los programas implementen de serie.

La noticia por tanto, no es tan catastrófica, aunque sí marcará tendencias. Lo que todavía no se sabe realmente, es si esta medida ayudará a paliar el phishing que sufre PayPal. A tenor del éxito del que todavía goza el phishing tradicional, los usuarios han demostrado que no se fijan realmente en los dominios, ni en

la autenticación SSL a la hora de introducir sus credenciales en cualquier página que se lo solicite.

Sergio de los Santos

16/05/2008 Preguntas frecuentes sobre el problema critptográfico de Debian

El problema encontrado en OpenSSL de Debian puede ser considerado, lamentablemente, un verdadero acontecimiento criptográfico. La criptografía es una ciencia compleja, y con el ánimo de aclarar las graves y extensas consecuencias del fallo, hemos redactado una serie de preguntas frecuentas para intentar, aun tratándose de un tema tan complejo, arrojar algo de luz.

¿Qué ha pasado exactamente?

Alguien (por error) del equipo de Debian eliminó una línea de código en el paquete OpenSSL de Debian que ayudaba a generar la entropía al calcular el par de claves pública y privada. Las claves sólo se calculaban tomando como semilla el PID del proceso. Al estar limitado a 32.768 semillas (tantos como PIDs de proceso son posibles) para la generación de números seudoaleatorios, el número de claves posibles es pequeño. Se han estado generando las mismas claves dentro de este número limitado de posibilidades desde septiembre de 2006. Como son pocas y de entropía pobre, se puede deducir la clave privada a partir de la pública porque el espacio de primos es muy pequeño y está precalculado. Ya se han generado listas disponibles para todos con la clave pública (del espacio a que han quedado limitado después del fallo) y su correspondiente privada. Para los usuarios de este OpenSSL de Debian sin entropía suficiente, se han roto las reglas de la criptografía asimétrica en la que por ahora confiamos todos y que sustentan las bases de la (poca) seguridad y confianza que pueda existir en Internet.

¿Es tan grave como parece?

Es más grave. Mucho más grave. Podríamos considerar que la criptografía de Debian en los últimos dos años ha sido una pantomima. Y es grave además porque no se resuelve por completo parcheando. Esa no es la solución definitiva. Hay que regenerar claves, revocar las antiguas, certificarlas en el caso de SSL, comprobar dónde fueron a parar claves generadas con Debian... No es un bug en un programa que eventualmente quedará obsoleto porque todo el mundo estará parcheado. Habrá administradores que no comprueben la debilidad sus claves, servidores SSL que jamás certifiquen de nuevo sus claves, claves perdidas de usuarios que dejen la puerta abierta a servidores SSH... También es grave porque arrastra a decenas de programas y sistemas que se valen de claves generadas con OpenSSL. SSL, SSH, OpenVPN, DNSSEC... Alguien lo ha calificado de "apocalipsis criptográfico". Además los principales perjudicados son los servidores que precisamente hayan buscado más seguridad con la criptografía de clave pública, porque contenían información crítica.

El SANS Internet Storm Center ha elevado el nivel de alerta general a 'amarillo'. No ocurre a menudo.

¿Cómo ha podido ocurrir?

Ha sido todo un desafortunado error. Aunque surgirán las teorías conspiratorias porque el código abierto ha estado ahí durante dos años, no ha sido hasta que Luciano Bello se ha dado cuenta que se ha corregido el fallo y se ha dado la voz de alarma. Pero el daño ya está hecho. Dos años de claves débiles generándose en cientos de miles de sistemas. Ha pasado desapercibido porque en general cualquier programa es

complejo, pero la criptografía lo es aún más. Además, Bruce Schneier dijo algo así como 'Good security looks the same as bad security' ('La buena seguridad se ve igual que la mala', frase aplicable aún más a la criptografía).

Kurt Roeckx fue quien planteó en un principio borrar líneas que consideraba problemáticas. Existe un correo de 2006 en una lista pública, en el que Roeckx plantea en una lista de OpenSSL qué pasaría si las eliminara. Pregunta si resultaría en una posible pérdida de aleatoriedad. La respuesta no oficial desde OpenSSL es que "no mucho" y que es partidario de borrarlas si ayuda en la depuración. Y era cierto, esas líneas no suponían problema: el problema es que en Debian se borraron más líneas de la cuenta, de las habladas en la conversación y para colmo los cambios no se enviaron a OpenSSL para que fueran revisados.

¿Se soluciona parcheando?

No. No se trata de un fallo de seguridad al uso. Ha existido una fuente de claves inseguras que se han esparcido durante dos años. Hay que comprobar y regenerar claves. El fallo fue anunciado a la vez que el parche, pero hay que tener en cuenta, que las primeras versiones de los parches para Debian y Ubuntu contenían regresiones. Han publicado nuevas actualizaciones para los propios parches que es necesario aplicar también.

¿Qué pasa si tengo un servidor web con acceso por HTTPS?

Si las claves han sido generadas con la versión de OpenSSL con el problema, las consecuencias son que alguien se puede hacer pasar por el servidor porque tendrá la privada de forma instantánea a partir de la pública. Además, cualquiera que haya tenido acceso a una conversación cifrada con el servidor, podría también descifrarla. Esto es así porque la clave simétrica que se utiliza para el cifrado ha sido intercambiada con la ayuda de claves asimétricas débiles. Un administrador debe además revocar la clave, generar una nueva, enviarla a la Autoridad Certificadora (que cobra por certificar) e instalarla. La catástrofe hubiese sito total, si una Autoridad Certficadora, hubiese generado claves y firmado certificados con estas claves débiles, pues el problema se extendería hacia abajo a todos sus clientes, en cuyos certificados ya no se podría confiar. Al parecer han comprobado que las principales Autoridades no se ven afectadas.

¿Qué pasa con SSH?

Los administradores que controlan sus sistemas a través de SSH se suelen autenticar a través de su clave privada y el servidor de SSH almacena la pública correspondiente. Esto es más seguro que usar una sola contraseña simétrica para autenticarse. El servidor cifra una cadena con la clave pública del que pretende autenticarse y se la envía, si puede descifrarla le deja pasar. En este caso puede que la clave pública sea realmente pública o no. En el primer caso, deducir la privada es instantáneo, y en el segundo caso, si no se conoce la pública, se debe hacer un ataque de fuerza bruta sobre un espacio de claves muy pequeño, algo que tarda unos 20 minutos con un ordenador de hoy día. Se ha creado un exploit para esto.

Todos los administradores que permitan a sus usuarios utilizar la clave privada para acceder a sus sistemas a través de SSH, deben auditar las claves para saber si son de las "débiles". Los administradores de SSH también se encuentran ante una tarea concienzuda, peligrosa, (y que deben emprender ya) incluso si no utilizan Debian, porque puede que sus claves hayan sido generadas en una distribución Debian y exportadas.

Los administradores de SSH comprobarán, con total seguridad, como los intentos de acceso ilegítimo se

multiplican en estos días.

¿A Windows le pasó lo mismo?

No. Se demostró que el generador de números aleatorios de Windows era débil, pero la diferencia es que según el estudio, había que conocer el estado previo del generador para saber el siguiente cálculo. Esto podría permitir descifrar conversaciones SSL entre dos sistemas. Pero para poder llegar a tener acceso a esa información inicial de la que se deducirían el resto de "estados del algoritmo", un atacante necesitaría poder tener acceso como administrador en el sistema. Digamos que para poder aprovechar el problema del algoritmo y poder descifrar la información, necesitaría tener el total control de la máquina para llegar a conocer un estado, con lo que el sistema ya estaría comprometido en sí.

Conclusiones

Lo peor no está ocurriendo ahora. Lo verdaderamente grave ha podido ocurrir antes (en los últimos dos años si alguien ha conocido este error y lo hubiese mantenido en secreto) y después (lo que nos espera a medida que se vaya descubriendo que sistemas importantes ha generado claves débiles).

Sergio de los Santos

20/05/2008 "Hoy goodware, mañana no sé"

Habían transcurrido sólo 6 horas desde que el responsable de seguridad de la multinacional había enviado al laboratorio un ejecutable para su análisis. Lo había encontrado en el portátil de un alto ejecutivo, durante una auditoría rutinaria. Desconocía el origen de aquel binario, no sabía lo que hacía. Cuando menos le resultaba sospechoso, la fecha de instalación coincidía con una salida del ejecutivo al extranjero donde, según los logs del sistema, había estado conectándose a Internet a través de al menos dos hotspots públicos. "¡Maldito WiFi!". Cuando recibió la llamada del laboratorio se apresuró a preguntar "¿malware o goodware?". La respuesta al otro lado del teléfono lo dejó algo desconcertado: "Hoy goodware, mañana no sé".

Y es que cualquiera que acuda a que le realicen un análisis de un binario espera un dictamen claro. O bien se trata de algún tipo de malware (virus, troyano, spyware, adware, etc.) que lleva a cabo acciones no deseadas en el sistema, o bien es goodware y por tanto no debemos temer de que realice ninguna trastada. Al fin y al cabo, un profesional puede realizar un análisis en profundidad del código mediante ingeniería inversa y saber exactamente como funciona y qué es lo que hace. ¿O no?

Tradicionalmente así solía ser. Un virus podía utilizar más o menos capas de ofuscación y cifrado, tener más o menos técnicas anti-debugging, podía ser más o menos complicado su análisis, pero al final, uno podía conocer al detalle como se comportaba. El virus era autónomo, todo su universo estaba autocontenido en su propio código. Eran otros tiempos, cuando los hombres eran hombres y se programaba en ensamblador.

Pero llegó Internet y lo cambió todo. Y no hablamos de la distribución masiva ni de los gusanos por Internet, ni de la explotación de vulnerabilidades mientras navegamos para infectar equipos de forma transparente, ni de la producción masiva de troyanos, ni siquiera del polimorfismo en origen a la hora de distribuir el malware, ni de las posibilidades de actualización y descarga de nuevas variantes, ni las botnets, etc. Las reglas han cambiado, y recién comenzamos a sufrir sus consecuencias.

¿Qué ocurre cuando no existe código malicioso en el binario? ¿Qué ocurre si tras un análisis al detalle de la muestra todo parece indicar que es goodware, o al menos hay ausencia de indicios que apunten a que es malware? Pues ocurre que puede ser goodware, o no. La clave está en que la lógica del malware, la inteligencia, se está trasladando a la parte servidor, allí donde queda fuera del alcance de nuestro análisis. ¿Cómo?.

Imaginemos que un espía profesional es contratado para atacar a un objetivo concreto. En vez de diseñar un malware tradicional, desarrolla una utilidad que, además de realizar su cometido, se conecta a Internet regularmente para comprobar si hay actualizaciones o para llevar a cabo cualquier otra acción común hoy día en el software. Una vez terminada la cuelga de Internet y, además, la envía a los laboratorios antivirus para su análisis. Esa muestra es analizada por los laboratorios y catalogada como goodware en su colección de binarios. Si algún día alguien envía de nuevo esa muestra, en sus registros ya se encuentra analizada y catalogada como goodware. Lógico, bastante tienen analizando todo lo que se produce nuevo como para estar reanalizando muestras.

La utilidad es pública, ha sido analizada por los laboratorios antivirus y se ha catalogado como limpia, de hecho no contiene ningún código malicioso oculto, además se la instalan indiscriminadamente los usuarios y tienen una buena experiencia (hace lo previsible). La utilidad se conecta regularmente a un servidor (del espía) en Internet para comprobar si debe autoactualizarse, descargando algún parche o nueva versión en caso necesario. Todo normal.

Pero hay un código que no sabemos que hace, el del servidor controlado por el espía en Internet. Allí tiene un script que recibe las consultas de la utilidad preguntando si hay alguna actualización, y una lógica que todo el mundo desconoce. El servidor devolverá o no un aviso de que hay una nueva actualización legítima pero, además, comprueba si la IP del sistema que está realizando la consulta pertenece al rango de la empresa objetivo; entonces, sólo entonces y en ese equipo concreto, descargará y ejecutará un código para robar información sensible.

Vale, bonita historia de espías. El problema es que lejos de ser una historia es un enfoque que va en aumento en el malware actual, y es posible que sólo estemos viendo la punta del iceberg.

Por ejemplo, en Hispasec estamos especializados en la detección y análisis de troyanos bancarios. Comienza a ser preocupante la aparición de familias que no son catalogadas como “bankers” por los antivirus, porque realmente no contienen código que pudiera hacer pensar que lo son. En todo caso son catalogadas como spyware, menos peligrosas, ya que su función consiste en enviar las URLs por las que navegamos a un servidor de Internet. La “gracia” está en que ese servidor sólo devuelve un nuevo código malicioso, o comandos interpretables por el propio malware, cuando la URL que envía al servidor coincide con la dirección de la web de una entidad bancaria determinada.

Estamos en un caso similar al del espía profesional, el análisis aislado del código que se instala en el cliente no puede dar pistas sobre la funcionalidad que puede adoptar ese binario. Un evento en concreto, en este caso visitar una URL determinada, es la que hace activar la lógica del servidor web que devuelve un nuevo código o instrucciones desconocidas hasta ese momento. Una lógica que puede o no estar activa en el momento en que se analiza la muestra, o incluso que puede tener más dependencias para activarse de forma que previene la detección de un análisis puntual.

Este traslado de la inteligencia del malware a la parte servidor supone nuevos retos y la necesidad de nuevos enfoques. En un momento en que también parte de la inteligencia de los antivirus se está externalizando en servicios en Internet, vemos que sigue siendo más importante que nunca tener inteligencia local, más

allá de las firmas de detección, que pueda identificar actividades sospechosas en nuestros sistemas. Y es que, al fin y al cabo, no hay balas de plata en esto de la seguridad, debemos seguir combinando diferentes capas complementarias de protección e ir evolucionando con los tiempos. Tenemos "diversión" para rato.

Bernardo Quintero

27/05/2008 Virus y promiscuidad. Del disquete al USB

A finales de la década de los 80 se empezaron a popularizar los virus del sector de arranque, que tenían la particularidad de que se propagaban a través de disquetes. Si introducías un disquete en un ordenador infectado el virus se copiaba al disquete, y a su vez ese disquete podía infectar cualquier otro ordenador donde fuera utilizado. A día de hoy vivimos una plaga del mismo perro con otro collar, al menos en la parte funcional. Con el disquete en desuso, las memorias USB han tomado el relevo como portadoras de una nueva generación de malware que aprovechan la "promiscuidad" con la que utilizamos el dispositivo.

¿Cuál es el dispositivo que más utilizas en ordenadores de terceros? Para muchos será la memoria USB, esa tan socorrida, que no dudamos en introducirla en cualquier ordenador. Para intercambiar documentos, para enseñar las últimas fotos, para llevarnos trabajo a casa, para que nos hagan una copia de ese programa, para una presentación, para pasarnos unos MP3,...

Tanto entrar y salir entre ordenadores diferentes no ha pasado desapercibido para los creadores de malware, que han visto en este dispositivo el transporte ideal para que sus bichos puedan saltar de un ordenador a otro. En un tiempo en el que, prácticamente, todo ordenador tiene conexión a Internet, y por tanto las distancias físicas son virtualmente inexistentes, esta nueva corriente nos traslada de nuevo a las infecciones de principios de los 90, basadas en la proximidad y la compartición de dispositivos de almacenamiento.
Una de las familias más representativas de esta nueva epidemia es denominada por los antivirus como "AutoRun", con el prefijo de "Win32" y/o "Worm". Como dato concreto, en VirusTotal se han recibido 7.742 variantes diferentes de esta familia (según MD5), sólo en lo que llevamos de mes de mayo.

El diseño de estos especímenes, que deberíamos catalogar como "gusanos" en vez de "virus" puesto que se reproducen con copias de sí mismos pero no pueden infectar a otros ficheros, es realmente simple. Toda la lógica se basa en aprovechar la funcionalidad AutoRun de Windows que automáticamente interpreta y ejecuta el archivo autorun.inf si se lo encuentra en el raíz de un medio removible, como un CD, DVD u otro tipo de memorias, incluyendo USB.

Los creadores de malware están aprovechando esta funcionalidad por defecto de Windows Explorer. Basta con introducir una memoria USB en un sistema para que automáticamente se ejecute el autorunf.inf que, típicamente, han diseñado para que lance a su vez un ejecutable con el código del gusano. El gusano se instala en el sistema e intenta copiar la pareja de ficheros, autorun.inf y ejecutable del gusano, en todas las unidades existentes. Esta forma de expandirse un tanto indiscriminada abarca la infección de discos duros, unidades de red, dispositivos removibles, etc, por lo que este tipo de gusanos se pueden encontrar más allá de en las propias memorias USB.

Las buenas noticias son que hay formas de intentar mitigar este tipo de gusanos configurando Windows para evitar el AutoRun automático, por ejemplo a través de la entrada del registro NoDriveTypeAutoRun. Sin embargo se ha detectado que la configuración de ese valor no es suficiente en Windows Vista para

prevenir la ejecución, debido a AutoPlay, otra funcionalidad por defecto.

Otro método más efectivo consiste en "trucar" Windows para que haga caso omiso de los archivos autorun.inf, indicándole que en vez de interpretar los comandos que incluya en su interior utilice unos valores alternativos, en concreto unos valores no existentes. Por lo que Windows no ejecutará nada.

Para ello se debe configurar una entrada en el registro de Windows. La forma más simple es copiar las siguientes líneas en el bloc de notas y guardarlas con la extensión .REG, por ejemplo noautorun.reg.

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

A continuación hacer doble click en el fichero noautorun.reg, Windows nos preguntará si estamos seguros de querer agregar esta información al registro, y elegiremos que Sí.

Recordar que con esta modificación también evitaremos la ejecución de los autorun.inf legítimos, por ejemplo esos que hacen que al introducir un CD o DVD automáticamente se ejecute un programa. En esos casos tendremos que hacer doble click en el programa para ejecutarlos. Si bien pensamos que esta "pequeña molestia" compensa si con ello evitamos la infección de nuestros sistemas.

Bernardo Quintero

22/07/2008 Descubiertos los detalles de la vulnerabilidad en el protocolo DNS

Desde el 8 de julio se está produciendo uno de los episodios más curiosos vividos nunca en la red. Se publicó ese día una actualización masiva para la mayoría de los dispositivos en Internet que utilizan DNS. Se dijo que había sido descubierta una vulnerabilidad que permitía falsificar las respuestas DNS, y por tanto redireccionar el tráfico. Casi todos los grandes y pequeños fabricantes y programadores actualizaron sus sistemas y se intentó mantener los detalles técnicos de la vulnerabilidad ocultos, por la gravedad y el potencial impacto que podría suponer. Finalmente, dos semanas después, se conocen los detalles.

Toda vulnerabilidad es importante y tiene un potencial impacto en la red. Sin embargo, cuando hablamos de la resolución de nombres y de problemas en los servidores DNS, la gravedad se multiplica porque se supone que los servidores DNS sustentan la red. Dan Kaminsky había descubierto un fallo de base en el protocolo que permitía a cualquiera falsificar las respuestas de un servidor. No era problema de ningún fabricante sino de casi todos, un fallo de diseño de un estándar usado en todo Internet. En un importante esfuerzo de coordinación todos los grandes fabricantes están publicado sus actualizaciones desde el día 8 de julio.

Pero Dan Kaminsky no daba detalles sobre el asunto. Era demasiado grave y pensaba que sería irresponsable proporcionar esa información sin dar suficiente tiempo a todos los administradores para actualizar. Del parche no se podía deducir el problema puesto que simplemente añadía aleatoriedad y entropía a ciertos valores que desde hace mucho se sabía que no eran la mejor solución para asegurar el protocolo. Es por esto que se apostaba desde un principio por que la vulnerabilidad de Kaminsky se tratara en realidad de una nueva forma más eficaz de engañar a los servidores DNS para que den respuestas falsas, gracias a un

fallo inherente del protocolo (y así ha sido).

Kaminsky daría los detalles un mes después, en la conferencia Black Hat de agosto. Por una parte, el descubridor estaba siendo responsable (dando tiempo a los administradores) pero tremendamente mediático por otra (creando una expectación exagerada en torno a la conferencia). Todo esto, ayudado por la desinformación de los medios generalistas ha ayudado a que la desconfianza siguiese creciendo. Todos defendían su teoría: desde el escéptico hasta el que hablaba de la debacle de la Red. Sólo un grupo de personas concretas conocía los detalles técnicos, y tenían instrucciones de no revelarlos y de evitar las especulaciones públicas. Kaminsky pretendía así ingenuamente asegurarse que sólo él daría los detalles cuando lo tenía planeado, cumpliendo así la segunda parte de su plan una vez publicadas las actualizaciones. Imposible... poco después las listas estaban llenas de comentarios y elucubraciones.

Afortunadamente en la seguridad informática siempre hay alguien que va más allá. Thomas Dullien, el CEO de la compañía Zynamics (también conocido como Halvar Flake) se aventuró a publicar en su blog su particular visión de lo que podía ser el problema descubierto por Kaminsky, sin tener conocimiento previo de los detalles. Y no se equivocó en su teoría. La insinuación de que estaba en lo cierto vino desde varios frentes (entre ellos desde un post en Twitter del propio Kaminsky), pero lo confirmó totalmente una entrada del lunes pasado en el blog de Thomas Ptacek, director la compañía Matasano que era de los que conocía los detalles reales. La entrada estaba firmada por un/a tal “ecopeland” del equipo de Ptacek. Según linkedin.com existe un/a Erin Ptacek (Copeland), desarrollador/a de software en Matasano (¿familiar del director?). En el post se daba la razón a Dullien, junto con todo lujo de detalles sobre el fallo que Dullien había ‘redescubierto’. La explicación fue retirada poco después (actualmente está disponible a través de la caché de Google). Ptacek se ha disculpado públicamente, probablemente se dejó llevar por su ánimo de compartir la información. Demasiado tarde... ya circula libremente por Internet.

Los detalles técnicos pueden ser encontrados en el apartado de más información. No tardarán en aparecer exploits. Ahora la gravedad del problema se multiplica. Afortunadamente casi todos los fabricantes han publicado ya un parche.

Aunque se conocía el problema desde enero, Kaminsky trabajó intensamente con los grandes fabricantes para mantenerlo en secreto y coordinar la aparición de parches un día concreto (que tuvo que coincidir con el día de actualización de Microsoft). Esto resulta extremadamente complicado, y hay que reconocer que ha debido resultar un trabajo complejo el coordinar y mantener la discreción sobre un tema tan delicado. Un esfuerzo elogiable. Sin embargo desde que se anunció la existencia del problema, sólo se han necesitado dos semanas para que sea desvelado, frustrando el plan de Kaminsky de aguantar un mes hasta la Black Hat para revelar los detalles.

Son muchas las moralejas y conclusiones que se pueden extraer de este incidente. De nuevo el debate sobre la revelación responsable de vulnerabilidades, la fuerza del ego de muchos investigadores, la demostración de que un esfuerzo coordinado para una actualización masiva ante un problema común es posible... pero sobre todo llama la atención la capacidad de Thomas Dullien de redescubrir un problema que siempre habría estado ahí, pero que no se había planteado buscar hasta que alguien apuntó que existía. Dullien contaba con las bases (el protocolo DNS sufre de problemas inherentes conocidos) sólo había que mover las piezas para encontrar lo que podía ser el fallo que otro decía ya saber. Y acertó. Una de las mejores formas de captar el interés de un asunto, (aunque siempre haya estado ante nuestras narices y creamos conocerlo) es afirmar que oculta un secreto.

Sergio de los Santos

30/07/2008 Consejos útiles contra el malware 2.0 en Windows

Los consejos obsoletos ofrecen una falsa sensación de seguridad de la que se están aprovechando los atacantes. Muchas de las informaciones publicadas sobre seguridad en general y sobre malware en particular no han sabido renovarse, y se perpetúan coletillas y axiomas que (aunque útiles y necesarios) no se han matizado ni completado correctamente con el tiempo. Son consejos de hace años, que no se han adaptado a una industria (la del malware) que avanza mucho más rápido de lo que podamos imaginar. Vamos a ofrecer algunos consejos útiles contra el malware... de hoy.

Administrador no, gracias

El principal consejo para los usuarios de sistemas operativos en general y los de Windows en particular es no usar la cuenta de administrador. Se debe utilizar la cuenta de un usuario sin privilegios, sin excusas. Esto es lo que puede llevar a una mayor protección no solo contra el malware, sino contra posibles despistes del propio usuario. Un "administrador" está precisamente para "administrar", y son muy pocas veces las que un usuario utiliza su sistema para realizar modificaciones importantes. La mayor parte del tiempo lee correo o navega, actividad esta última que conlleva un importante riesgo, sea con el navegador que sea. Esta irresponsable actitud de usuario administrador perpetuo está heredada de los tiempos de Windows 9x. No tenía sistema de usuarios local real, ni soportaba NTFS, con lo que no se podían establecer permisos por usuarios. Cuando apareció XP, tras su instalación Microsoft permitía por fin la creación de un usuario distinto al administrador para el uso del sistema. Un gesto que hubiera servido de algo si este mismo usuario no perteneciese por defecto al grupo administradores, y por tanto fuese tan poderoso como él.

A nadie que utilice un sistema operativo que no sea Windows se le ocurre realizar sus actividades cotidianas como "root" o súperusuario. En Windows, lo extraño es precisamente lo contrario, trabajar con cuentas limitadas. Este es el verdadero origen de la mayor parte de los males, y de que el malware pueda campar a sus anchas en un ordenador donde puede escribir, leer, modificar... puesto que es ejecutado con los mismos permisos del usuario que está usando la máquina.
En Windows Vista, Microsoft ha establecido un importante sistema de seguridad para mitigar este problema heredado, rompiendo así una tendencia muy arraigada y limitando el poder del usuario habitual. Se ha relegando por fin el uso del administrador a un segundo plano. Sin embargo esto ha sido visto por muchos usuarios como un estorbo, en vez de como una importantísima mejora en su seguridad.

Aunque se presente aquí como panacea, no lo es. Todavía una parte del malware actual podría seguir actuando. Además, trabajar como usuario raso en XP o 2000 puede llegar a ser incómodo, incluso para usuarios experimentados. Es necesario tener conocimientos sobre permisos, privilegios, NTFS, derechos, herencias, grupos... Por si fuera poco, con ánimo de no complicar al usuario, Windows XP Home Edition escondía deliberadamente la pestaña de seguridad para poder cambiar los permisos, a no ser que se trabajara en modo a prueba de fallos.

Actualizar el sistema

No sólo Windows, sino todos los programas que tengamos instalados deben estar actualizados a la última versión de su rama. Esto es muy importante, pues una gran parte del malware hoy en día se aprovecha de vulnerabilidades conocidas que ya tienen parche. Muchos usuarios piensan que un Windows parcheado tendrá problemas "legales" o que sufrirá fallos de compatibilidad. Un Windows sin actualizar es un Windows contaminado. Pero no sólo el sistema operativo. Todo programa es susceptible de sufrir problemas de seguridad y de que sean aprovechados. Desde el reproductor de MP3 hasta el lector de PDF, se han detectado ataques dirigidos a versiones vulnerables de los programas más utilizados para tareas

comunes. La única solución es no abrir archivos no solicitados tengan el formato que tengan y sobre todo, mantener actualizados los programas que los interpretan.

Mantenerse informado

Mantenerse informado sobre tendencias de seguridad, malware y estado en general de la seguridad en la red. No se puede luchar contra lo que no se conoce. Son muchos los usuarios que desconocen que pueden ser infectados por archivos que no son ejecutables, que es posible ejecutar código arbitrario en el sistema de forma transparente con sólo visitar una web, o que el SSL del banco visitado no tiene por qué significar que un sistema no esté troyanizado o que no se trate de un phishing. Otros piensan que el hecho de que la página del banco aparezca modificada y requiera más casillas de la tarjeta de coordenadas de lo habitual, significa que la seguridad ha aumentado...estar informado es primordial. No sólo por lo cambiante de algunas técnicas, sino también porque es necesario seguir de cerca ciertas campañas que emprenden los atacantes y que suscitan modas y comportamientos sobre los que resulta imprescindible estar especialmente atento. Existen momentos en los que se perpetran ataques concretos para los que puede que la única solución sea conocerlos y evitarlos hasta que exista parche.

Otros consejos

Estos tres consejos anteriores son los más importantes. Por desgracia no son los que se dan habitualmente en los medios no especializados. Ni la tecnología, ni Internet ni los atacantes son los mismos que hace cinco años, por tanto las precauciones no deben ser iguales para siempre. Obviamente es necesario usar herramientas o suites de seguridad actualizadas (cortafuegos, antispyware...) pero sobre todo, saber cómo se usan. Si no se saben manejar, se vuelven inútiles.

¿Y el antivirus? Por supuesto. También es imprescindible tener un antivirus actualizado a diario.

Sergio de los Santos

20/10/2008 La comparativa del escándalo

Secunia ha publicado una comparativa de suites de seguridad que ha levantado cierta polémica. Especialmente por la metodología escogida: en vez de utilizar distintos tipos de muestras de malware (como viene siendo lo habitual para comprobar los ratios de detección), se han usado exploits creados para la ocasión y páginas web modificadas para aprovechar estos exploits. Las casas antivirus no han salido muy bien paradas, pero en realidad es necesario matizar en extremo las conclusiones de esta comparativa.

Las condiciones

En total se han usado 300 exploits (144 archivos maliciosos y 156 páginas web modificadas). Los resultados dicen que ninguna de las suites consiguió el aprobado.

De acuerdo con Secunia, las condiciones de los tests fueron las siguientes:

1- Los archivos maliciosos fueron primero analizados al desempaquetar un archivo ZIP, en el que estaban contenidos, para comprobar la eficiencia del escáner al acceder en “tiempo real”.

2- Posteriormente la carpeta fue escaneada de forma manual para asegurarse de que fueran procesados todos los archivos.

3- Las páginas web maliciosas fueron analizadas una por una usando Internet Explorer.

Solo la suite de Norton, de las 12 analizadas, pasaba del 20% de detección, mientras que el resto no llegaba al 3%. Pero esto no significa nada.

Las quejas

Muchas casas antivirus y empresas del sector no están de acuerdo (con razón) con los resultados obtenidos. Utilizan los siguientes argumentos:

* Los tests no se realizaron de forma completa. Lo ideal hubiera sido tener una máquina en la que estuvieran instaladas tanto la versión vulnerable del software a explotar como la suite de seguridad de Internet. El paso siguiente es intentar ejecutar el exploit en ese entorno y esperar a ver si es bloqueado o no.

* Los tests se realizaron a demanda, es decir, se pasó el escáner sobre los archivos que contenían los exploits, pero no se ejecutaron. La única forma de detección posible, en esas circunstancias, es que exista una firma específica en el componente antivirus para detectar los exploits o que sean detectados por heurística.

* Se han utilizado exploits de laboratorio, especialmente creados para estos tests y diferentes de los que podrían circular por Internet en la actualidad.

Por estas y otras razones alegan que el test puede ser orientativo únicamente a nivel del escáner, pero en ningún momento se puede juzgar la totalidad de la suite por los resultados obtenidos. También se defienden diciendo que, muchas de las características anti-exploit incluidas en las suites ni siguiera han entrado en juego, como son por ejemplo:

* Virtualización y mecanismos de protección contra desbordamientos de búfer/pila/heap.

* Incluso si los exploits fueran ejecutados, un HIPS (sistema de prevención de intrusiones basado en host), un IDS (sistema de detección de intrusos) o un firewall podrían servir para bloquearlos.

* Tampoco se ha tenido en cuenta el filtrado de URLs maliciosas ni de exploits del navegador.

El CEO de AV-Test.org Andreas Marx, también apunta que falta información técnica sobre cómo se ha realizado el test, tal como por ejemplo: productos exactos y versiones utilizadas, fecha de la última actualización de los motores, o bajo qué entorno se han realizado las pruebas sobre las páginas web y HTML.

La conclusión del informe, firmada por Thomas Kristensen, el CTO de Secunia: “Los resultados muestran que los fabricantes de productos de seguridad no se centran en vulnerabilidades. En vez de eso, tienen un enfoque mucho más tradicional, lo que deja a sus clientes expuestos al nuevo malware que explota vulnerabilidades. (...) El área está, más o menos, completamente ignorada por los fabricantes de productos de seguridad”.

Esta conclusión, junto con la omisión de ciertos detalles, no ha sentado nada bien a algunas personas

influyentes dentro del sector y ha provocado las siguientes reacciones:

* Alex Eckelberry de Sunbelt Software: “Este test es estúpido y una maniobra publicitaria inútil”.

* Pedro Bustamante de Panda Security: “Es como decir que vas a probar el ABS de un coche tirándolo por un acantilado de 200 metros de profundidad. Absurdo, sensacionalista y como mínimo engañoso”.

A todo esto, Kristensen se ha defendido, diciendo que: “Las Internet Security Suites son bastante útiles para la mayoría de usuarios. (...) Pero es mejor prevenir los ataques parcheando que confiar en otras medidas de seguridad por sí solas”.

Nuestras conclusiones

Es necesario resaltar además algunos aspectos interesantes que observamos en este informe:

* Está realizado desde una compañía que vende servicios de prevención de vulnerabilidades. Por tanto la conclusión extraída le es conveniente desde el punto de vista comercial. Lo que es peor, está enfocada desde todos los aspectos para que así sea. Por ejemplo: los exploits más usados por los atacantes sí suelen ser más reconocidos por las firmas de las soluciones antivirus que, obviamente, los creados para la ocasión. Esto no es nada nuevo, pasa exactamente igual con el malware: desde siempre, los virus recién creados ha sido menos detectados por firmas en un principio. Tampoco es difícil crear específicamente troyanos “no detectados por firmas. Los atacantes lo hacen todos los días. Otra cosa es que sean detectados por comportamiento en el sistema una vez ejecutados, que es el punto fuerte de las suites en estos momentos.

* Las alegaciones desde las casas antivirus son legítimas. No es ningún secreto que el modelo de detección por firmas es cada vez “una parte más” de los antivirus, y no se puede juzgar a un producto exclusivamente por la detección estática de muestras. Es lo mismo que ocurre con VirusTotal. Los resultados obtenidos al enviar una muestra son analizados de forma estática, por tanto pueden diferir de lo que un usuario obtiene con el antivirus instalado en su sistema. Las suites, cada vez más, se basan en el comportamiento de las muestras para detectar el malware, además de en las firmas. Es más, hacen una buena labor en ese sentido, y no es posible hoy en día evaluar un producto completo sólo por una de sus funciones. Si se quiere evaluar la calidad y cantidad de firmas, se debe ser consciente de que eso es sólo una parte del producto.

* Sí es cierto que el usuario medio suele ser víctima del marketing agresivo de las casas antivirus, y creen que la suite les salvará de todo mal. Slogans como “Protección total” o “Blindaje del sistema” calan en el usuario que concluye que realmente es lo único que necesita. Por otro lado, este tipo de informes como el generado por Secunia polarizan la opinión: “¿Acaso, a pesar del dinero invertido en la solución antimalware, no estoy protegido por completo?” o “Las soluciones antimalware no sirven para nada”. Ninguna de las dos posiciones es adecuada. Las soluciones antivirus son imprescindibles, pero es necesario combinarlas con otros métodos de prevención como son las actualizaciones de seguridad de los sistemas y programas, además del uso de cuentas no privilegiadas.

Pablo Molina

27/11/2008 El antivirus que lo detecta todo

No es broma, las nuevas estrategias en la detección de código malicioso apuntan a ese objetivo que puede sonar utópico. No quiere decir que nos estemos acercando al antivirus perfecto, sino que los nuevos enfoques de las soluciones de seguridad intentan identificar tanto al malware como a los ficheros legítimos, tratan de clasificar todo.

Si nuestro ordenador fuera una discoteca el antivirus sería el portero, el encargado de decidir quién puede pasar y quién no a divertirse en nuestro local. Dependiendo de lo exclusiva que sea nuestra discoteca, la dirección podría haber ordenado al portero que siguiera una de las siguientes estrategias:

(1) sólo dejar pasar a las personas VIP y conocidas según una lista (lista blanca).

(2) no dejar pasar a aquellas personas reconocidas como problemáticas (lista negra).

Con la estrategia (1) nuestra discoteca sería demasiado elitista, ya que no permitiría entrar a gente nueva o desconocida hasta que no hubiera sido dado de alta en la lista blanca. Un verdadero incordio y no sería operativo. En el caso (2) nuestro local estaría más animado y evitaríamos a los individuos peligrosos reconocidos, que en un principio no eran demasiados, así que la dirección de la discoteca apostó por esta opción.

El de los antivirus siempre había sido un mundo de listas negras, estrategia número (2), con firmas y patrones para detectar al código malicioso e impedirles que pudieran entrar o ejecutarse en nuestro ordenador.

Con el tiempo se vio que esa estrategia era insuficiente, ya que había mucho malware de nueva creación que no se encontraba en la lista negra (se les colaban muchos indeseables). La lista negra requería ser constantemente actualizada y, aun así, no era suficiente. Se apostó por potenciar la heurística, que en el caso de nuestro portero vendría a ser una orden similar a la siguiente:

(3) no dejar pasar a personas que por sus características te parezcan sospechosas o que pudieran causar problemas

Con la entrada de la heurística la discoteca tuvo algunos problemas, el portero sospechó de gente VIP y no les dejó entrar. Así que la dirección le dijo al portero que utilizara también una pequeña lista blanca para reconocer a esas personas y no impedirles su entrada por error. De esta forma el portero comenzó a utilizar al mismo tiempo las estrategias (1), (2) y (3) de forma complementaria.

De esta misma forma el uso de listas blancas comenzó a ser más popular entre los antivirus, si bien solía limitarse a corregir y prevenir falsos positivos, para no dar por malware o virus un fichero legítimo muy conocido. Ya sabéis, detectar como malware el notepad.exe sería como negarle la entrada a nuestra discoteca a Pilar Rubio. Imperdonable.

Pasó el tiempo y la discoteca seguía teniendo incidentes y problemas de seguridad. Aun teniendo una lista negra, heurística y lista blanca, seguían colándose muchos indeseables al local. La dirección pidió al portero que aumentara su nivel de heurística, más paranoia a la hora de impedir el paso a personas que aparentemente pudieran dar problemas.

En el mundo de los antivirus hemos visto ese aumento de paranoia en heurísticas más agresivas, por

ejemplo aquellas que detectan como malware un fichero por el simple hecho de estar tratados con un "packer".

Con la nueva heurística más paranoica aumentaron las reclamaciones a la dirección de la discoteca. A muchas personas que no eran tan famosas como para estar en la lista VIP o pequeña lista blanca se les negaba la entrada al local por parecer sospechosas a ojos del portero.

La discoteca estaba en crisis. Si aumentaba la heurística y paranoia del portero tenían reclamaciones por impedir la entrada a personas legítimas. Si disminuía la heurística se le colaban demasiados indeseables.

En esa situación se encuentra la industria antivirus actual: una lista negra actualizándose constantemente (hay antivirus que se actualizan varias veces cada hora); una heurística agresiva para detectar nuevos especímenes que no estén en su lista negra; y una lista blanca más pequeña, y que se actualiza menos, para evitar meter la pata excesivamente detectando como malware algún software muy conocido y/o extendido. El resultado es de crisis técnica, siguen teniendo muchos problemas como en la discoteca, o bien están detectando como malicioso software legítimo, o bien se les sigue colando en cantidad malware de verdad, o en el peor de los casos ambas cosas.

Una de las soluciones podría ser tener una lista blanca muy grande y actualizarla constantemente, como en el caso de la lista negra. Eso limitaría el número de falsos positivos y las heurísticas podrían concentrarse en aquellos ficheros totalmente desconocidos, que no están ni en la lista negra ni en la lista blanca, y que deberían ser un número más reducido.

De esta forma un antivirus podría tener un primer dictamen muy rápido dado un fichero: o se encuentra en la lista negra y por tanto es malicioso, o se encuentra en la lista blanca y no necesito analizarlo, o lo marco como desconocido "lista gris" y le aplico una heurística agresiva, o les hago un seguimiento especial (monitorización del comportamiento), o lo paso a cuarentena a la espera de un proceso que permita tener un dictamen más o menos fiable.

Esta nueva estrategia requeriría manejar unas listas blancas y negras muy grandes, y actualizarlas constantemente, para minimizar el número de ficheros que podrían caer en la lista gris (desconocidos). Eso se traduce en el consumo de un mayor número de recursos por parte del antivirus local: imaginemos que el portero tiene que consultar dos listados de millones de registros cada vez que alguien quiere entrar a nuestro local. En el PC significaría mayor consumo de memoria y CPU, amén de una constante actualización de los ficheros de firmas a través de Internet.

La solución a este problema de recursos viene de la mano de lo que se ha dado por llamar "cloud computing", tan de moda desde hace un tiempo, y que no es más que traspasar parte del trabajo a un servidor remoto con una enorme capacidad de almacenamiento y proceso (lo que se conoce por "la nube"). En vez de tener que consultar unas enormes listas negras y blancas en el ordenador local, con el consiguiente consumo de recursos, esa consulta se hace a través de Internet a un gran servidor centralizado (un cluster de servidores) que devuelve al PC el resultado, si ese fichero está en su lista negra o blanca.

Con este enfoque el número de ficheros desconocidos disminuye y, por tanto, el antivirus local puede centrarse en ellos con heurísticas o una monitorización del comportamiento con mayor detenimiento para dictaminar si es un código malicioso o no. La otra ventaja es que ese dictamen local puede traspasarse a la nube, a los servidores centralizados, en tiempo real, de forma que ese malware nuevo descubierto en un PC formará parte de la lista negra y prevendrá a otros sistemas que realicen a posteriori una consulta sobre ese fichero en particular. Incluso, dependiendo de la estrategia del antivirus, los ejecutables

desconocidos podrían ser enviados al servidor centralizado donde podría ser analizado automáticamente con mayores recursos informáticos o ser trasladado a un analista humano si el dictamen automático no es concluyente.

Esta realimentación constante, entre PCs y servidores centralizados que permite el “cloud computing”, está produciendo listas negras y blancas con millones de firmas o registros que serían inviables tener de forma local en un PC, y nos acercan un poco más a la utopía del antivirus que es capaz de detectar casi todo.

No sería de extrañar que a corto o medio plazo, dado un análisis a demanda de un disco duro, un antivirus pudiera llegar a darnos un log completo (identificando todos los ficheros), indicando cuales son benignos según su lista blanca, cuales son malware según su lista negra, y aplicando un coeficiente de mayor o menor peligrosidad según heurística a los archivos desconocidos.

Volviendo a nuestro portero, imaginemos que la discoteca ha contratado un sistema de reconocimiento facial que conecta automáticamente a un servidor centralizado que mantiene una gran base de datos de personas y sus antecedentes. Una cámara en la puerta automáticamente va capturando imágenes de las caras de las personas que quieren entrar, las envía al servidor centralizado donde se compara con su base de datos, y devuelve al portero en tiempo real si es alguien de confianza, si es alguien problemático, o si no tiene información de esa persona.

El portero puede ahora, de forma instantánea, permitir o denegar la entrada según la respuesta del sistema, y sólo tendrá que utilizar su heurística con unas pocas personas (las que el sistema no reconozca). Al ser pocas personas a las que debe aplicar la heurística podrá hacerlo con más detenimiento, desde pedir documentación a cachearla, actuaciones que antes no podía realizar de forma indiscriminada por un problema de volumen y recursos. Si detecta que un desconocido lleva un arma, además de impedirle la entrada al local, se informa automáticamente al servidor centralizado que mantiene la base de datos, realimentando el sistema.

Como el mismo servidor centralizado da servicio a muchas discotecas, el sistema se alimenta de la información y actuaciones individuales de muchos porteros en tiempo real. Además recoge información adicional que puede ser útil a la hora de correlacionar datos.

Visto así esta estrategia parece un avance importante para el mundo de lo antivirus, pero no es la panacea. El problema sigue siendo el mismo, dictaminar si un fichero es malicioso o no. Incluso puede que los errores al dictaminar sean más graves, si marcamos por error que un archivo es benigno y se cataloga en la lista blanca es más que probable que se deje actuar a ese código en cualquier ordenador local a sus anchas o, en el mejor de los casos, aplicándole análisis heurísticos o de comportamiento más relajados en el sistema local. Imaginemos un delincuente que está marcado como confiable en el sistema de reconocimiento facial, entraría a todas las discotecas automáticamente y el portero no se molestaría en prestarle mayor atención.

Los servidores centralizados deberían tener mecanismos de reanálisis y depuración de sus clasificaciones, para detectar errores tanto de malware que se haya asignado a las listas blancas como de software legítimo que han entrado por error en las listas negras. Tarea no sencilla si tenemos en cuenta los volúmenes en los que pueden moverse las colecciones de ficheros, lo que implica automatización y por ende dictámenes con un margen de error no despreciable.

Por lo tanto estos nuevos antivirus que tienden a intentar identificarlo todo, tanto el malware como los

ficheros legítimos, no necesariamente tienen que ser más fiables. Una cosa es que lo identifiquen todo o casi todo, otra cosa es que esa identificación sea correcta. Lo que si es cierto es que las estrategias basadas en el "cloud computing" suponen un plus importante en la detección del malware, especialmente con especímenes muy nuevos, dada la actualización en tiempo real de las bases de datos que se consultan y la correlación centralizada de datos que se puede realizar gracias a la realimentación constante que producen los antivirus conectados al servicio.

En definitiva, el "cloud computing" y el uso masivo de listas blancas son una capa más a sumar al antivirus tradicional, pero no deberían por si solos convertirse en solución de seguridad. Sus beneficios se pueden notar ya en las primeras soluciones antivirus que lo están implantando, sus debilidades tampoco se harán esperar.

Bernardo Quintero

Oficina de Hispasec actualmente











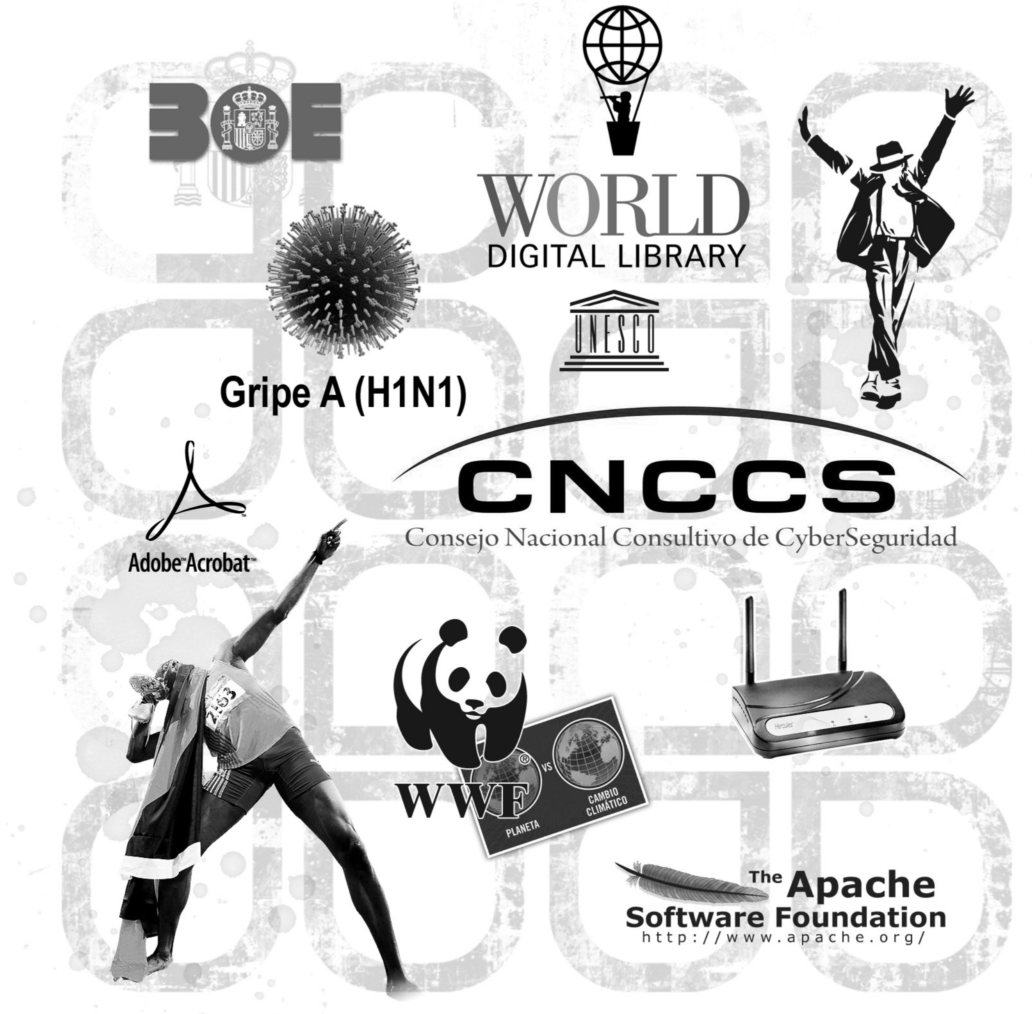
Capítulo 11

AÑO 2009

7D9

3731

11111011001



1230768000 – 1262303999

Durante este año...

_ El 1 de enero **desaparece oficialmente la edición en papel del BOE español** (Boletín oficial del Estado) después de publicarse durante 350 años. Queda solo la versión digital con pleno valor jurídico y un ahorro de 6 millones de euros al año. Las visitas a la web del BOE crecen a un ritmo del 20% anual, con una media de tres millones de visitas.

_ La **guerra de Gaza** continúa con el ejército israelí invadiendo por tierra la franja de Gaza. Acaban los seis meses de alto el fuego. Unos días antes, los israelíes usaron las fuerzas aéreas para bombardear a los palestinos. El 10 de febrero se celebrarían las elecciones en Israel.

_ Durante enero, la crisis continúa derrumbando (metafóricamente) bancos y grandes entidades. A finales de enero **cae el sistema bancario de Islandia**. El primer ministro Geir Haarde dimite y es sustituido por Jóhanna Sigurðardóttir, declarada abiertamente gay.

_ Durante febrero se propagan **los fuegos en Australia**, que llegan a matar a 173 personas y herir a 500.

_ El 28 de marzo se declara **"La hora del planeta"**. La WWF anima a todos los ciudadanos, empresas y gobiernos a combatir el cambio climático apagando las luces durante una hora. Así, a las 20:30 CET se apagan las luces de cientos de lugares públicos en todo el planeta, dejando sin iluminación monumentos y edificios emblemáticos.

_ El 2 de abril **se reúne de nuevo el G-20 para discutir sobre la crisis económica mundial**. Se congregan en Londres los responsables financieros de los 20 países más relevantes del planeta. España acudió a la primera gracias al líder francés Sarkozy, que cedió a José Luis Rodríguez Zapatero una de las sillas que le correspondían en la primera reunión en Washinton.

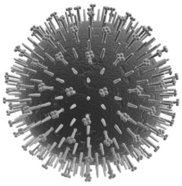
_ El 7 de abril se sentencia a **Alberto Fujimori** a 25 años de prisión por ordenar secuestros y asesinatos desde sus fuerzas de seguridad.

_ El 21 de abril la UNESCO lanza la **World Digital Library**. La Biblioteca Digital Mundial pone a disposición en Internet, de manera gratuita y en formato multilingüe material literario de la mayor parte de las culturas de todo el mundo. Según la propia página, los objetivos de la Biblioteca Digital Mundial son: Promover el entendimiento internacional e intercultural, ampliar la cantidad y la variedad de contenidos culturales en Internet, facilitar recursos a los educadores, estudiosos y el público en general y permitir a las instituciones asociadas reducir la distancia digital dentro de y entre los países.

_ El 25 de mayo, La República Democrática y Popular de Corea (RDPC, Corea del Norte) realiza con éxito **un nuevo ensayo nuclear** subterráneo en el marco de sus "medidas destinadas a reforzar sus capacidades de disuasión nuclear". Toda la comunidad internacional rechaza de pleno estas pruebas. El primer ensayo nuclear del país en octubre de 2006, según el ministerio ruso de defensa, era de entre 5 y 15 kilotones. Se afirma que este es entre 4 y 6 veces superior en potencia.

Gripe A.

A comienzos de marzo, más de la mitad de los residentes de La Gloria, en el Estado de Veracruz en México, sufre problemas respiratorios derivados de una gripe. El pueblo está localizado cerca de un inmenso criadero de cerdos que produce anualmente un millón de cabezas. Comienza la pandemia de lo que finalmente **se denominó Gripe A**.



Gripe A (H1N1)

El nombre oficial es Influenzavirus A de origen porcino (subtipo H1N1). Al ser descubierta se le denominó gripe porcina aunque no fue el único nombre que se manejó. La Organización Mundial de la Salud Animal propuso "gripe norteamericana". La Unión Europea quiso llamarla "nueva gripe". Finalmente el 30 de abril de 2009 la Organización Mundial de la Salud (OMS) decide denominarla gripe A (H1N1), zanjando la cuestión y resultando el nombre mayoritariamente aceptado. Se comienzan a detectar casos de infecciones en personas que no han viajado a Méjico, con lo que se concluye que se transmite entre humanos. El número de casos aumenta en todo el mundo. Muchos afectados con otras afecciones respiratorios mueren a causa de la gripe. Las alarmas se disparan. El 29 de abril, la OMS incrementa el nivel de alerta por pandemia a 5 indicando que la pandemia es "inminente". El 11 de junio, se declara la fase 6 de alerta, esto es, pandemia. Esto indica que la gripe se propaga mundialmente de forma rápida, no que sea más virulenta. De hecho, se registran en menos de dos meses casos en todos los continentes. Los países compran grandes cantidades de vacunas de cara a una posible infección masiva con la llegada del otoño.

_ El 25 de junio muere **Michael Jackson**, icono mundial del pop. Las primeras noticias sobre su muerte aparecen en Twitter. La red se colapsa buscando información sobre el artista, las páginas de información no dan abasto. Youtube muestra todos su vídeos una y otra vez. Se le homenajea con páginas como www.eternalmoonwalk.com, donde cualquier usuario puede colgar vídeos haciendo el "moonwalk" y son encadenados. Decenas de miles de personas participan el en proyecto. Las empresas aprovechan para relanzar su discografía y apenas dos meses después se estrena una película documental "This is it" sobre su vida. Como suele ser habitual, a las pocas horas aparecen correos con malware que prometen más información sobre su muerte.



_ Explota la crisis política en **Honduras**. Durante la madrugada del 28 de junio, fuerzas armadas al mando del teniente coronel Rene Antonio Herpburn Bueso se introducen por la fuerza en la residencia presidencial y detienen y exilian al presidente Manuel Zelaya. Toda la comunidad internacional condena enérgicamente el **golpe de estado**. Le siguen multitudinarias manifestaciones a favor del gobierno de Roberto Micheletti. Zelaya se recluye en la embajada de Brasil en Honduras.

_ El 5 de agosto, la **Wikipedia** en español alcanza los 500.000 artículos.

_ El 16 de agosto el jamaicano **Usain Bolt bate el récord del mundo de los 100 metros lisos** con una marca de 9,58 segundos durante el Campeonato Mundial de atletismo en Berlín. Desde los tiempos de Carl Lewis y Ben Johnson a finales de los 80, una carrera de velocidad no ofrece tanta expectación. Después de 20 años en los que un puñado de hombres le robaban, literalmente, centésima a centésima al cronómetro, aparece Bolt y baja en dos años 16 centésimas al récord inmediatamente anterior.

9,79 segundos. Ben Johnson en 1988. Anulado por dopaje.
9,86 segundos: Carl Lews en 1991
9,85 segundos: Leroy Burrel en 1994
9,84 segundos: Donovan Bailey en 1996
9,79 segundos: Maurice Green en 1999
9,78 segundos: Tim Montgomery en 2002
9,77 segundos: Justin Gatlin en 2006
9,74 segundos: Asafa Powell en 2007
9,69 segundos: Usain Bolt en 2008
9,58 segundos: Usain Bolt en 2009.

_ A pesar de los esfuerzos de todos los madrileños por acoger los **Juegos Olímpicos de 2016**, Rio de Janeiro se erige como la capital donde se realizará el evento. Madrid sale a la calle los días previos a la decisión para apoyar su candidatura.

_ El 15 de septiembre muere **Patrick Swayze**, a los 56 años.

Seguridad Informática



_ **Conficker**, también conocido como Downadup, salta a los medios generalistas activando alarmas. Es la última alerta sobre malware masivo. La combinación de ciertas técnicas le permite conseguir un buen número de infecciones. Conficker juega bien sus cartas, haciendo un inteligente uso del Autorun y Autoplay de Windows para difundirse. Igualmente, utiliza técnicas avanzadas de criptografía e ingeniería social, y sale a la luz en un momento oportuno: aprovecha una vulnerabilidad en Microsoft Windows muy reciente, y por ello encuentra un gran número de sistemas vulnerables en los que expandirse. Igualmente, evoluciona lo suficientemente rápido como para corregir sus propios errores y mantenerse como uno de los ejemplares más infecciosos. Es el primero en usar un algoritmo de generación de dominios que, por los números usados, impide virtualmente que los investigadores puedan adelantarse al registro de dominios "nodriza" y estudiar su comportamiento. Desconcierta a todos porque lo más curioso es que no parece tener un fin concreto más allá de su propia expansión. Todo ello a pesar de una implacable persecución de los antivirus que, aunque no tardan en detectarlo, parecen no ser efectivos contra su difusión. Con el tiempo, obligaría a Microsoft a replantearse su política de ejecución automática de dispositivos extraíbles, publicando un parche que restringiría la ejecución de archivos por defecto.

_ Se detecta en enero **malware oculto en una copia pirata de Apple iWork 09 para Mac OS X**. Sigue la intención de la industria del malware de llegar a los Mac OS X. Apple reacciona tímida y casi de forma ridícula, incluyendo un rudimentario antivirus en su versión Snow de septiembre de ese mismo año. Tan rudimentario que parece reconocer solo dos familias de malware que suele atacar al sistema operativo de Apple y solo comprueba las descargas por Safari. No limpia el sistema ni nada parecido, solo aconseja de la peligrosidad del archivo. Es un movimiento que causaría cierta sorna entre la industria antivirus. Realmente es un gesto que debe valorarse positivamente, pero de poca utilidad real.

_ En febrero Apple publica uno de sus habituales mega parches para Mac OS X 10, incluyendo además actualizaciones para Safari bajo Windows y Java para Mac. Corrige 50 vulnerabilidades diferentes. El descubridor de una de ellas se queja de que han tardado **más de seis meses en publicar una**

actualización para un grave problema en Safari, que permitía a un atacante tener acceso a ficheros locales del sistema a través de una página web.

_ La ShadowServer Fundation advierte el día 19 de febrero de una potencial vulnerabilidad en Adobe Acrobat Reader que podría permitir a un atacante ejecutar código arbitrario. Al descubrirse el problema mientras estaba siendo aprovechado activamente por atacantes, se convierte en **un grave 0 day**. Adobe reconoce finalmente la vulnerabilidad como una nueva amenaza, para la que no existe parche disponible. Tres semanas después, publican un parche pero no para todas sus versiones mantenidas. En abril Adobe confirmaría **otra grave vulnerabilidad en Adobe Reader** que estaba siendo aprovechada por atacantes para ejecutar código en el sistema (tanto Windows como cualquier otro sistema operativo que lo soporte). En VirusTotal.com se detecta claramente la tendencia al alza de análisis de archivos PDF en las horas en las que se hace público el problema, sin duda motivados por la alerta generada en torno a ese 0 day. Si la media diaria recibida en VirusTotal.com está entre 150 y 200 archivos en formato PDF, el día del anuncio se superan los 500 archivos analizados. En octubre, se repetiría la historia: se encuentra el enésimo 0 day en Adobe Reader para Windows.

_ Moxie Marlinspike demuestra en una conferencia en la Black Hat cómo **eludir la autenticación y el cifrado SSL de las páginas supuestamente seguras**. El investigador se centra en una inteligente combinación de técnicas que permiten confundir a los usuarios (incluso a los avanzados) sobre si están o no en la página correcta. Ninguna de las técnicas usadas es realmente nueva, pero todas en conjunto forman una excelente herramienta llamada sslstrip.

_ En febrero, **Microsoft reconoce en una nota oficial que está investigando la existencia de una nueva vulnerabilidad en Office Excel** que podría permitir la ejecución remota de código si un usuario abre un archivo Excel especialmente manipulado. En la entrada titulada "Detection Added For The New 0-day In Excel" del blog de investigación y respuesta ante amenazas del Microsoft Malware Protection Center se añade algo de información adicional. Se proporciona una pequeña lista con los hashes SHA1 de algunos de los archivos que contienen el exploit. Haciendo una búsqueda de los hashes en VirusTotal.com se aprecia que uno de los archivos fue enviado y analizado por primera vez en diciembre de 2008, dato indicativo de que una primera versión del exploit podría estar siendo utilizada desde entonces. Poco después Microsoft sufriría otro grave problema de seguridad en PowerPoint, descubierto mientras estaba siendo aprovechado por atacantes.

_ En marzo, Matthew Dempsky se lleva 1.000 dólares por encontrar un **pequeño fallo de seguridad en djbdns**. D. J. Bernstein programó a mediados de los noventa, qmail y djbdns con la seguridad siempre en mente. Precisamente, estaba harto de vulnerabilidades en sus homólogos Sendmail y BIND, dos pesos pesados de Internet que sufrían de enormes agujeros de seguridad cada muy poco tiempo por aquel entonces. Como alternativa, creó estos servidores siguiendo unas premisas muy sencillas en las que se premiaba por encima de todo la seguridad y simplicidad. Estaba tan seguro de su trabajo que ofreció una recompensa económica a quien encontrara fallos en su software. Hoy en día es habitual que premien económicamente a los que encuentran fallos de seguridad, pero por entonces, era una especie de osadía. Para Bernstein se convirtió en su garantía de seguridad. Nunca se pensó que pasarían tantos años hasta que alguien pudiese hacerse con el premio.

_ **Rutkowska** y su equipo publican el documento técnico **"Attacking SMM Memory via Intel CPU Cache Poisoning"**. System Management Mode (SMM) se refiere a un modo de operación más privilegiado en las arquitecturas x86. El SMM podría considerarse el Ring -2. SMM se ejecuta en la zona de memoria conocida como SMRAM. Se supone que el controlador de memoria solo debe permitir al firmware (la BIOS) acceder a esa zona de memoria. Una vez que la BIOS carga en esa parte el SMM, sólo el código

que esté en ese "anillo" debería poder acceder a él. Lo que descubren es cómo acceder a esa zona, bajar dos niveles desde el Ring 0 (a través de un driver en el sistema Windows, o incluso siendo root en Linux) y ejecutar código con los privilegios de SMM. Con todo ese poder, una vez más y como ya demostró con Blue Pill, se puede crear un rootkit indetectable. Literalmente, el sistema operativo e incluso los drivers, todo, podría estar bajo el control de un atacante y hacer creer una total "mentira" al sistema basada en una ejecución de código capaz de controlar al más bajo nivel el sistema.

_ Guido Landi hace públicos (sin previo aviso) los detalles **de una vulnerabilidad que permite la ejecución de código en la nueva versión 3.5 de Mozilla Firefox** con solo interpretar un archivo XML especialmente manipulado. En principio la prueba de concepto publicada hace que el navegador deje de responder, pero es posible de forma relativamente sencilla modificar el exploit para que permita la ejecución de código. El problema afecta a todas las versiones (actual y anteriores) del navegador sobre cualquier sistema operativo. Firefox no tarda en corregirlo.

_ La universidad de Toronto publica un documento de investigación sobre **GhostNet**, una botnet concebida para un objetivo muy concreto: el espionaje. La población de GhostNet es de solo 1.295 sistemas infectados, pero la novedad es el objetivo político que persigue.

_ En abril se habla en los medios de que los malos están pagando **hasta 25.000 euros por un modelo antiguo de móvil Nokia** 1100 (de 2003). La razón es que dicen que contiene un error que permitiría interceptar los SMS, y poder así eludir la seguridad de los bancos que utilizan este método para validar transacciones. El tema levanta mucho revuelo pero pronto queda en el olvido.

_ En mayo se descubre **una vulnerabilidad "como las de antes"** en Internet Information Server, el servidor web de Microsoft y, lo peor, aprovechando fallos y problemas que parecían pertenecer ya al pasado, como de otro tiempo. El fallo dispara el número de "desfiguraciones" (defaces) en servidores web con IIS. La vulnerabilidad combina elementos que dieron muchos dolores de cabeza a Microsoft a finales de los 90. El fallo está en IIS 6.x a la hora de procesar peticiones HTTP especialmente manipuladas con la cabecera "Translate:f" y con caracteres Unicode. Un atacante podría eludir la autenticación (y subir ficheros si lo permiten los permisos) al disparar un problema de validación en WebDAV. En IIS 5.x, la vulnerabilidad es más grave. Poco después se encontraría una nueva vulnerabilidad en el FTP de Microsoft IIS 5 que permitía la ejecución de código. Mal año para IIS, que había conseguido muchos meses de relativa tranquilidad en cuestión de seguridad.

_ A pesar de que en la última macro-actualización de Mac OS X corrige 67 vulnerabilidades, **Apple deja sin solución un grave problema en el JRE** (Java Runtime Environment) que puede ser aprovechado por atacantes para ejecutar código con solo visitar una página web, conocido desde agosto de 2008.

_ Tras la sucesión de graves vulnerabilidades, exploits 0 days y críticas vertidas hacía la política de seguridad de Adobe, anuncia que en agosto **comenzará a aplicar un ciclo de publicación de actualizaciones de seguridad** igual al de Microsoft, es decir, los segundos martes de cada mes y fuera de ese ciclo aquellas que por su importancia o gravedad precisen de una actuación inmediata. Se ve obligada a sacar parches fuera de su ciclo nada más empezar, en mayo y más tarde en julio.

_ Otro **0 day en Microsoft DirectX** golpea a Microsoft. Poco después, de nuevo se descubriría otro en Microsoft Office Web Component.

_ Durante el verano, el Consejo Nacional Consultor sobre CyberSeguridad (CNCCS) apoya la iniciativa parlamentaria que propone la creación del Plan Europeo de CyberSeguridad en la Red, una organización

privada que tiene, como miembros fundadores, a **Panda Security, S21Sec, Hispasec Sistemas y Secuware**. Poco después el Senado la aprueba por unanimidad. La misión del CNCCS es poner a disposición de las diversas organizaciones que operan en España, gubernamentales o no, el conocimiento y experiencia de sus miembros en asuntos relacionados con la cyberseguridad nacional o global, con el fin de hacer más segura Internet y las redes de Información, a la vez que potenciar la innovación y el crecimiento económico. En septiembre se unirían CNCCS: Cybex, Amper, Telefónica, TBSecurity, Barcelona Digital Centro Tecnológico, Universidad de Deusto Laboratorio S3Lab, Colegio Oficial de Ingenieros de Telecomunicación (COIT) y AEDEL.

_ Unos investigadores australianos descubren una nueva combinación de métodos para **provocar colisiones en el algoritmo de hash SHA1** de forma mucho más rápida. Sólo se necesitarían 2^{52} intentos. Esto podría resultar en ataques prácticos posibles a este sistema de hash. A principios de 2005 un grupo de investigadores chinos consiguió reducir el número de intentos para acelerar el proceso de colisión de dos mensajes cualesquiera a 2^{69}. Poco después se avanzó hasta 2^{63}. El departamento de algoritmos y criptografía de la Universidad de Macquarie (Australia) lo reduce a una complejidad de 2^{52}.

_ Adobe reconoce **distribuir una versión vulnerable de Adobe Reader** desde su página oficial. Confiaban en que el usuario actualizase más tarde, una vez descargado e instalado.

_ Tanto Microsoft como Adobe **reconocen solucionar dos fallos que se convierten en 0 day, pero que en realidad conocían desde 2008**. Esto es una práctica habitual, pero el problema en este caso es que, antes de solucionarlos, otros investigadores con no muy buenas intenciones acaban por descubrirlos también y aprovecharlos en beneficio propio. Esto les obliga a sacar un parche con mayor celeridad, aunque llevasen meses con la vulnerabilidad "aparcada".

_ A finales de agosto **se optimiza el ataque a WPA para reducirlo a un minuto**. Se trata de un escenario totalmente teórico, casi irreal, pero mejora el tiempo del ataque que se describió el año anterior sobre WPA, pero que necesitaba de unos 15 minutos para poder introducir con éxito pequeños paquetes falsos en el tráfico.

_ Los servidores de la **fundación Apache** presentan durante algunas horas una escueta página informando que se encontraban investigando **un incidente en sus servidores**. Aclaran que no se trata de un exploit que afectase al popular servidor web, producto de la propia fundación, sino de una llave SSH comprometida. La llave en cuestión permitía el acceso a una cuenta para efectuar copias de respaldo automáticas del sitio web "ApacheCon", en una máquina situada en un alojamiento externo a la fundación. Esta máquina fue usada para subir archivos a un servidor de su infraestructura, denominado minotaur. apache.org, con funciones notables, como proveer de cuentas para los "comitters" (cuentas con acceso de escritura a los repositorios de código) y de entrada a los distintos sitios web de la fundación Apache. Apache gestiona el fallo de forma totalmente transparente, admitiendo errores y aciertos.

_ En septiembre, Laurent Gaffié detecta **un fallo de seguridad en Windows Vista** que podría permitir a un atacante provocar un BSOD (pantallazo azul, una denegación de servicio) con solo enviar algunos paquetes de red manipulados a una máquina que tenga activos los servicios de compartición de archivos **(protocolo SMB2)**. El fallo (incomprensiblemente simple) está en el intérprete de las cabeceras SMB, concretamente en el driver srv2.sys. El ataque es tan sencillo que recuerda a los "pings de la muerte" que hicieron estragos a finales de los 90 en los sistemas Windows. Poco después se descubre que la ejecución

de código es posible y se hacen públicos varios exploits.

_ Cisco y Microsoft publican parche para la vulnerabilidad **"Sockstress"**, revelada en octubre de 2008. Son los primeros de una larga lista de fabricantes que se ven afectados por esta vulnerabilidad.

_ Hispasec lanza un estudio comparativo: **¿Cuánto tardan los grandes fabricantes de software en arreglar una vulnerabilidad?** Nos preguntamos cuánto tardan 10 grandes fabricantes en solucionar una vulnerabilidad cuando no sufren la presión de los medios, cuando el fallo es solo conocido por ellos y quien la ha descubierto. Cómo reaccionan ante esta situación "ideal" (desde su punto de vista), en la que la vulnerabilidad les ha sido comunicada en secreto, y ambas partes acuerdan no hacerlo público hasta que exista una solución. Algunas de las conclusiones del estudio de 449 vulnerabilidades son que **la media de los grandes fabricantes es de seis meses para solucionar una vulnerabilidad**, independientemente de su gravedad. Encontramos ejemplos en los que una vulnerabilidad crítica es solucionada un año después de ser descubierta, y otros en los que se tardan apenas unos días. Todos los datos y el informe completo, están disponibles de forma totalmente gratuita y sin necesidad de registro desde:

http://www.hispasec.com/laboratorio/Hispasec_Estudio_Vulnerabilidades.pdf

_ Se celebra con éxito la **LaCon 2009**, su segunda edición. Charlas entretenidas, interesantes, novedosas... y políticamente incorrectas.

_ Aparece **URLZone, un troyano peculiar que abre nuevas técnicas innovadoras en el mundo del malware**. El troyano es capaz de recordar el balance anterior de su víctima, y falsearlo en la cuenta una vez ha sido robado. Así, el usuario no percibe que está siendo víctima de fraude. No puede detectar la falta de dinero en su cuenta a menos que analice un extracto por algún otro medio que no sea su propio ordenador troyanizado, o le sea devuelto algún recibo. Además, cuando URLZone detecta que no está en su botnet "legítima", o sea, la red de sistemas infectados que reciben órdenes de uno o varios sistemas centrales, modifica su comportamiento para eludir a los investigadores. Si es instalado en un laboratorio, y la red central no "conoce" a ese sistema, simulará un comportamiento extraño, en el que toda persona que haya recibido dinero de la cuenta de la víctima, parecerá que es el mulero de turno. De paso, ocultan así las cuentas de los muleros reales, y perseguir el dinero se convierte en una tarea todavía más compleja.

Una al día

11/02/2009 Por qué el 92% de las vulnerabilidades críticas en Windows minimizarían su impacto si no se usase la cuenta de administrador

BeyondTrust ha emitido un escueto informe en el que afirma que el impacto del 92% de las vulnerabilidades críticas en Windows se minimizaría si no se usasen los privilegios de administrador. El uso de la cuenta de administrador, como ya hemos defendido desde aquí en otras ocasiones, es uno de los más graves problemas con los que se enfrenta Microsoft y que el propio Windows ha ayudado a alimentar con versiones

anteriores. Veremos contra qué tipo de vulnerabilidades protege el principio de mínimo privilegio y por qué, en realidad, el informe no descubre nada nuevo: el principio de mínimos privilegios es una regla que siempre ha estado ahí para todos los sistemas operativos... menos para los de Microsoft.

BeyondTrust ha publicado un estudio pormenorizado de todas las vulnerabilidades publicadas por Microsoft en 2008. Ha concluido que el 92% de las vulnerabilidades críticas y el 69% de todas (críticas o no) serían menos graves, o tendrían un impacto mucho menor, si fuesen aprovechadas por un atacante pero la víctima no fuese administrador. Cuando un atacante aprovecha una vulnerabilidad de ejecución de código en un programa que está siendo usado por un administrador, éste código hereda sus permisos y el atacante podrá campar a sus anchas (como el usuario) en el sistema una vez explotado el fallo. En un 92% de los casos, según el informe, se hubiese limitado considerablemente la gravedad del asunto.

Desde Hispasec siempre se ha recomendado evitar la cuenta administrador, es el principal consejo para los usuarios de sistemas operativos en general y los de Windows en particular. Esta es la primera capa de seguridad con la que se debe proteger un usuario. Un "administrador" está precisamente para "administrar", y son muy pocas veces las que un usuario utiliza su sistema para realizar modificaciones importantes. La mayor parte del tiempo lee correo o navega, actividad esta última que conlleva un importante riesgo, sea con el navegador que sea. Esta irresponsable actitud de usuario administrador perpetuo está heredada de los tiempos de Windows 9x. No tenía sistema de usuarios local real, ni soportaba NTFS, con lo que no se podían establecer permisos por usuarios. Con XP, por fin, Microsoft permitía la creación de un usuario inicial distinto al administrador para el uso del sistema, pero lo incluía por defecto al grupo administradores y por tanto no lo protegía ni limitaba en absoluto.

El otro 8%

El informe no explica por qué el impacto de tantas vulnerabilidades es susceptible a la cuenta bajo la que se exploten. ¿Por qué no nos protege del 100% de las vulnerabilidades críticas el hecho de trabajar como usuario sin privilegios? Pues porque el resto, el 8% de vulnerabilidades se pueden clasificar básicamente en tres:

* Las que permiten revelación de información. Estas suelen ser independientes del usuario bajo el que se explota la vulnerabilidad.

* Las que afectan a servicios de sistema que corren siempre bajo cuentas privilegiadas. Los servicios especiales de sistema corren normalmente bajo la cuenta SYSTEM. Si un atacante aprovecha un fallo en estos servicios desde el exterior, no hay nada que el usuario pueda hacer para evitarlo excepto intentar precisamente que el servicio no esté accesible para cualquiera. Hay que recordar que ya hicieron un trabajo importante de limitación de cuentas de servicio cuando apareció XP. En 2000 todos los servicios trabajaban con los máximos privilegios. En XP y 2003, no.

* Las elevaciones de privilegios. Evidentemente, este tipo de vulnerabilidades permiten precisamente saltar de una cuenta sin privilegios a otra con mayor capacidad de actuación sobre el sistema. Si se trabaja con cuenta limitada, es una de las mayores preocupaciones. Si se trabaja como administrador, estas vulnerabilidades no suelen tienen impacto (excepto si logran privilegios de SYSTEM, ligeramente superiores a los del propio Administrador). Hoy en día, las vulnerabilidades de elevación de privilegios son poco valoradas por los atacantes (en especial los creadores de malware) porque presuponen (y presuponen bien) que su víctima será administrador.
¿Windows un 92% más seguro?

Significa que el trabajar con cuentas con privilegios menos elevados ayudaría a que el sistema fuese un 92% más seguro? Desgraciadamente no, pero sin duda ayudaría.

Trabajar como usuario con pocos privilegios no es la panacea. Trabajar como usuario raso en XP o 2000 con cierto software puede llegar a ser incómodo, incluso para usuarios experimentados (y casi siempre esto es responsabilidad de los propios programadores, que no suelen tenerlo en cuenta). Es necesario tener conocimientos sobre permisos, privilegios, NTFS, derechos, herencias, grupos... Por si fuera poco, con ánimo de no complicar al usuario, Windows XP Home Edition esconde deliberadamente la pestaña de seguridad para poder cambiar los permisos, a no ser que se trabajara en modo a prueba de fallos. En otros sistemas operativos resulta más sencillo, porque los programadores siempre han supuesto que su usuario no iba a gozar de todos los permisos.

El problema es, como de costumbre, la educación del usuario ante una estructura tan compleja como hoy en día es un sistema operativo. Estamos tan mal acostumbrados que si un usuario de cualquier sistema operativo (distinto a Windows) se convierte en víctima del exploit de una vulnerabilidad, y por ello el sistema queda totalmente comprometido, lo primero que preguntamos es si estaba trabajando como root. Si es así, inmediatamente la mayor parte de la responsabilidad cae del lado del usuario (abstrayéndonos de la responsabilidad del software). Se entiende como una especie de castigo justo por no conocer y limitar convenientemente su entorno de trabajo, o por despiste. En Windows, si un usuario es víctima de un malware que se le ha colado a través del navegador, y esta víctima trabaja como administrador (lo más habitual) el problema se achaca directamente al sistema operativo o al navegador y sus continuos fallos. No solemos pararnos a pensar en que el usuario, tampoco en este caso, conoce realmente su entorno de trabajo o no se le han proporcionado la facilidades para hacerlo, y por eso no lo ha limitado convenientemente. Limitándolo, si bien no se reduciría el número de fallos, sí se degradará considerablemente su impacto, como bien recuerda el informe.

Sergio de los Santos

18/03/2009 Antivirus y falsos positivos... un desmadre

A Fred Cohen se le conoce como el padre de los "virus informáticos", por ser el primero en acuñar este término en la década de los 80 para describir a estos programas. Además de bautizarlos y analizarlos, en su estudio "Computer Viruses - Theory and Experiments" llegaba a la conclusión de que no existía algoritmo que pudiera detectar todos los posibles virus. Cuando ahora se cumplen 25 años de su estudio podemos decir que Cohen tenía razón y que, además, vamos a peor. Vale que no podamos detectar todo el malware pero, por favor, no detectemos a los que no lo son.

A lo largo de toda la historia del malware (los virus tienen menos de 30 años, lo que nos quedará aun por ver) las conclusiones de Cohen han pesado como una losa. A diferencia de hace unos años, donde todavía existía publicidad engañosa con aquello de "100% contra virus conocidos y desconocidos", a día de hoy quién más y quién menos no le queda más remedio que esconder sus vergüenzas. Todos asumimos que los antivirus son otra capa de seguridad que pueden minimizar nuestra ventana de amenazas, pero que en última instancia siempre estamos expuestos a sufrir una infección.

Esa conciencia sobre las limitaciones de las soluciones de seguridad y la exposición al riesgo es buena y deseable, porque permite educarnos en un uso más profiláctico de la informática, aplicando más capas de seguridad adicionales o simplemente mejorando nuestros hábitos diarios. De modo que es bueno que seamos conscientes de que nuestro antivirus sólo nos protege contra el 80% de las amenazas que

potencialmente podemos recibir, quién dice 80% puede decir 65%, o 50%... pero bueno, al fin y al cabo, nos está protegiendo.

¿Realmente los porcentajes de detección pueden llegar a ser tan bajos? No, según el caso pueden ser aun peor. En los últimos tiempos existe un problema de escalabilidad en la detección de malware, simple y llanamente, los laboratorios antivirus no dan a basto con la producción actual de bichos nuevos. Si en febrero de 2004 podíamos leer en el recién estrenado blog de F-Secure: “Dos nuevas variantes de Bagle han sido avistadas. Otra vez. Parece que tendremos un fin de semana ocupado”, ¿qué tendrían que decir hoy en cualquier laboratorio antivirus donde se reciben a diario miles de nuevas variantes de malware?.

Está claro que la opción de escalar el problema aplicando a los métodos de análisis tradicionales una regla de tres no es buena, si se han multiplicando por miles los especímenes diarios que puede recibir un laboratorio la solución no es multiplicar por mil los analistas. Entre otras cosas porque el negocio de los antivirus dejaría de ser rentable. Así que ahora se trabaja mucho en la automatización de análisis y heurísticas para aumentar los ratios de detección. El efecto secundario de esta automatización y heurísticas más agresivas es que los antivirus tienen un mayor número de falsos positivos, es decir, se equivocan más al detectar como malware algo que en realidad no lo es.

Esta problemática, lejos de ser una anécdota, es cada vez más preocupante. Ya la hemos tratado en una-al-día anteriormente, y vamos a peor. En Hispasec recibimos día sí, día también, mensajes de desarrolladores preguntando o quejándose de que los antivirus de VirusTotal están detectando como malware su software legítimo, con las interferencias y problemas que ello les causa ante sus clientes y su reputación global. Nosotros mismos hemos sufrido en propias carnes que VTuploader, la herramienta para enviar ficheros a VirusTotal, fuera detectada hace unas semanas, teniendo que solicitar la corrección de las firmas a los antivirus implicados.

Algo está fallando en los antivirus cuando, incluso, están aumentando los falsos positivos con los propios ficheros legítimos de Windows. Se supone que comprobar la no detección de componentes de Windows debe ser la medida más básica de control de calidad antes de publicar una nueva actualización.

Estamos ante una carrera loca por ver quién detecta mayor número y más rápido (de lo que sea), y nos estamos olvidando de que, ante todo, un antivirus no debería molestar ni interferir (demasiado) en el normal funcionamiento de los sistemas y los programas legítimos. Un usuario o una empresa puede llegar a entender que un antivirus no detecte todos los virus del mundo, incluso que se le cuele alguno que otro, pero difícilmente podrá aceptar que el antivirus le cuelgue el ordenador, borre ejecutables que no debe, o impida la ejecución de una aplicación corporativa.

No todo vale para detectar más. Estamos perdiendo el foco. Es un desmadre.

Bernardo Quintero

25/03/2009 Routers, modems y botnets

Desde hace unas semanas DroneBL ha sufrido un ataque distribuido de denegación de servicio procedente de una botnet llamada ‘psybot’. Nada nuevo si tenemos en cuenta que DroneBL ofrece un servicio gratuito de publicación de listas negras de IP en tiempo real, lo cual no es precisamente una manera de ganarse admiradores entre las filas de creadores de malware, spammers, etc. Lo interesante del asunto se lo encontraron cuando recabaron información sobre su atacante.

El gusano que teje 'psybot' no tiene como objetivo los ordenadores personales o servidores. El binario ni tan siquiera está compilado para la omnipresente arquitectura x86. Su foco de infección se encuentra en los routers y modems ADSL con Linux y procesador MIPS. El gusano efectúa un barrido por rangos de IP escaneando los puertos 22, 23 y el 80, buscando una vulnerabilidad que expone la administración remota del dispositivo a través de telnet, ssh e interfaz web inclusive con los permisos por defecto. Si la configuración ha sido modificada, lo intentará por fuerza bruta.

Tras obtener una shell con permisos de administrador borra el archivo '/var/tmp/udhcpc.env' que pertenece al cliente DHCP y comprueba la existencia del comando wget para efectuar la descarga de una réplica del gusano con el mismo nombre y ruta que el archivo borrado. Tras ello inyecta reglas en iptables para cerrar la entrada en los puertos 22, 23 y 80 y así evitar su apertura lícita y reinfección. Una vez infectado, el nuevo nodo, conecta a un servidor IRC donde procesa el topic que contiene instrucciones para los bots.

Aunque el primer contacto con esta botnet fue documentado por un tal Terry Baume en enero de este año, parece ser que este es el primer ataque a gran escala o el incidente que ha tenido mayor repercusión mediática hasta el momento. Varios son los factores que no pasaron por alto los creadores de 'psybot', un vector fácil, contraseñas por defecto y exposición de la administración remota, una presa descuidada, como un olvidado router con el que no se interactúa y se mantiene encendido las 24 horas, y sobre todo el silencio: ¿Cuándo fue la última vez que monitorizaste el tráfico del router?

David García

02/04/2009 Éxitos y fracasos de Conficker

Si algo ha conseguido Conficker, es generar expectación mediática (incluso que le dediquemos varias una-al-día). Alentado por las casas antivirus, que no pasan por su mejor momento en nivel de detección global, Conficker ha servido para recordar al mundo que existen todavía amenazas globales en forma de malware con nombre y apellido. Conficker, cabeza de turco frente a otros tipos de malware anónimos y mucho más peligrosos, ha gozado de algunos éxitos rotundos, tanto mediáticos como técnicos que vamos a repasar.

Éxitos mediáticos

* Poco queda del Conficker original que apareció en noviembre. Se ha convertido, como todo malware 2.0 que se precie, en una sofisticada red de sistemas y servidores, como ocurrió con el Storm Worm. Alguien a quien señalar con el dedo y que recuerde al público (consumidor de software) que las casas antivirus siguen ahí. El miedo incita a protegerse.

* Conficker se ha centrado, durante mucho tiempo, más en la expansión que en el ataque. Se ha dedicado a recopilar máquinas infectadas sin un fin concreto (al menos que conozcamos por ahora). Este pequeño misterio ha atraído la atención de las casas antivirus, y por tanto de los medios.

* El éxito incluso le ha llegado de formas muy retorcidas. La proliferación de programas legítimos y específicos para desinfectar el sistema ha plagado las primeras búsquedas de Google de software falso. Es fácil encontrar con cualquier buscador, malware que dice ser un limpiador de Conficker.

* Establecer una fecha de apocalipsis vende mucho. Como hicieran el virus Viernes 13, Michelangelo... recuerda viejos tiempos, siempre mejores para las casas antivirus. Se dijo que el 1 de abril Conficker se activaría y colapsaría muchas webs. Nada ha ocurrido, como era de esperar. Es imposible que algo que

genera tanta expectación cause un gran impacto. La gente tiende a prepararse para mitigar el ataque. Cuando algo viene por sorpresa, cuando no hay fecha establecida, es cuando el impacto se puede considerar verdaderamente serio.

Éxitos técnicos

* El mayor éxito de expansión de Conficker ha sido a través de las memorias USB. Pero no solo el hecho de adoptar esa estrategia, sino cómo lo ha hecho. Por primera vez, creó un archivo autorun.ini funcional pero disimulado con basura, que conseguía pasar desapercibido. Logró saltarse los métodos básicos de bloqueo de autoejecución de Windows.

* Siguiendo con el autorun, pudo disimular su ejecución mostrándose como la exploración de carpetas. Es un engaño muy conseguido. El uso de contraseñas por defecto también proporcionó numerosas alegrías a los atacantes.

* Uno de los éxitos técnicos más curiosos ha sido el uso de miles de dominios. El malware actual suele contener un algoritmo interno para generar dominios aleatorios (que probablemente no existen), desde donde descargarán nuevas funcionalidades. Los atacantes compran los dominios y cuelgan en ellos la actualizaciones para que el malware salga a buscarlas cuando los genere internamente. Cuando un laboratorio consigue descifrar ese algoritmo de generación, suele adelantarse a los atacantes y registrar ellos mismos esos dominios. Así podemos saber, según las visitas que reciba el dominio, el número de infectados. Normalmente el malware genera un número manejable de dominios cada día, y los atacantes registran solo algunos. Aunque se descifró el algoritmo de generación de dominios de Conficker, este pasó a generar 50.000 dominios aleatorios (de 4 a 9 letras) al día. Tanto dominio, por supuesto haría que muchos de los generados coincidiesen con dominios ya registrados y legítimos que todos los sistemas infectados visitarían. Los medios advirtieron que Internet se colapsaría por esta razón el 1 de abril.

Fracasos técnicos

* Pocos. Prácticamente su único problema ha sido la detección. Toda versión conocida de Conficker es detectada normalmente por más del 90% de los motores que alojamos en VirusTotal. Las casas se han volcado con él y lo detectan casi unánimemente. Es por eso que Conficker, aunque interesante, pasa automáticamente a ser una amenaza de mucho menos calibre. ¿Qué hubiera pasado si a pesar de toda esa cobertura mediática, los niveles de detección fuesen bajos? No es posible esta combinación. Cuanto más se hable de un malware, más detectado es. La pregunta es qué hubiera ocurrido sin esta cobertura mediática. La respuesta es que los niveles de detección hubieran sido mucho menores, y la infección mucho más discreta y mayor. En otras palabras, lo mismo que está ocurriendo ya con el resto del malware industrial, mucho más abundante, que se crea hoy en día. Los verdaderamente peligrosos que no aparecen en titulares.

Porque, ¿qué puede resultar más peligroso?, este ejemplar:

http://www.virustotal.com/analisis/963521ca26f84db93146f0b7891d0f1f

o este:

http://www.virustotal.com/analisis/07cd5b586a82487949ba18d03bdab8c7

El primero es un Conficker detectado por el 95% de los motores. El segundo es un troyano especialmente

destinado al robo de contraseñas, que lleva más de un mes en nuestra base de datos. En ningún momento ha sido detectado por más de dos motores.

Conficker es peligroso, no cabe duda, es una grave plaga que hay que combatir. Pero no es el único malware contra el que se debe luchar.

Sergio de los Santos

21/06/2009 Protegiéndonos de las soluciones de seguridad

Acabo de recibir un mensaje de una gran consultora, de esas que hacen estudios basándose en estadísticas tras recopilar la opinión de terceros supuestamente expertos. Muy amables, solicitan corrija una errata en una de las respuestas que rellené en su cuestionario. La pregunta pedía que, según mi criterio, enumerara el top 10 de amenazas de seguridad a las que se deberían enfrentar las empresas a corto y medio plazo. La respuesta que suponen una errata es: las soluciones de seguridad.

Supongo que la mayoría estamos de acuerdo en que, en casos puntuales, una solución de seguridad puede introducir nuevas amenazas, bien por mal funcionamiento en sus funciones de protección, bien por nuevas vulnerabilidades que se derivan del propio producto o servicio de seguridad. No obstante, incluir esa remota y puntual posibilidad en un top 10 de amenazas no es muy acertado. Así que entono el mea culpa por una mala descripción de lo que quería decir (tampoco había mucho espacio en el campo de texto libre del cuestionario), y les voy a enviar la rectificación: marketing falso en soluciones de seguridad.

En su día me molestaba mucho leer el eslogan de "100% de protección contra virus", una herencia de aquella molestia se puede encontrar aun hoy día en el aviso que escribí hace 5 años en la web de VirusTotal: "No existe solución en el mundo que pueda ofrecer un 100% de efectividad en el reconocimiento de virus y malware en general. Si le ofrecen un producto con el 100% de efectividad, está siendo víctima de publicidad falsa.". Afortunadamente el marketing de los antivirus ha evolucionado y ya nadie se atreve a decir nada parecido.

Sin embargo, en términos generales, el marketing en las soluciones de seguridad sigue siendo poco honesto, tanto con el usuario final como con el cliente corporativo. Un buen momento que tengo para afianzar esa sensación es cuando presento los resultados de auditorías y test de penetración a clientes corporativos. Es entonces cuando escucho frases como: "pero el vendedor nos dijo que este sistema de prevención de intrusiones evitaba cualquier tipo de inyección", "no puede ser, el portátil tiene un sistema de cifrado y nos dijeron que era imposible extraer ninguna información", etc.

Ya sabemos que cualquier solución de seguridad que nos ofrezcan, u ofrezcamos, no es perfecta. Así que el vender las soluciones de seguridad exagerando sus virtudes y omitiendo sus debilidades podría entenderse como picaresca, parte del juego entre vendedor-comprador. Pero los efectos en realidad son mucho más perniciosos que el del anuncio del detergente que nos asegura que lava más blanco que ninguno, porque puede llegar a crear una falsa sensación de seguridad en el comprador y las consecuencias pueden ser desastrosas para la empresa.

No se trata simplemente de que el comprador haya adquirido una solución que no es la mejor de su categoría, como ocurre en el caso del detergente, sino que probablemente no le hayan explicado las limitaciones de esa tecnología y de la que adolece cualquier otro producto de la misma categoría. El resultado es que el comprador no entenderá la necesidad de añadir capas adicionales de seguridad para proteger sus activos,

una verdad que en el mejor de los casos descubrirá durante una auditoría o test de penetración, y en el peor de los escenarios ya sería demasiado tarde.

Mi humilde consejo: cuando intenten venderle una tecnología o solución de seguridad, desconfíe de cualquier presentación que no incluya explícitamente una descripción de sus debilidades o limitaciones.

Bernardo Quintero

Sergio de los Santos
Diseño: Alberto García

1998 - 2009

Una al día

Once años de seguridad informática

Anuario ilustrado de seguridad informática, anécdotas y entrevistas exclusivas... Casi todo lo que ha ocurrido en seguridad en los últimos once años, está dentro de “Una al día: 11 años de seguridad informática”.

Para celebrar los once años ininterrumpidos del boletín Una al día, hemos realizado un recorrido por toda una década de virus, vulnerabilidades, fraudes, alertas, y reflexiones sobre la seguridad en Internet. Desde una perspectiva amena y entretenida y con un diseño sencillo y directo.

Los 11 años de Una al día sirven de excusa para un libro que está compuesto por material nuevo, revisado y redactado desde la perspectiva del tiempo. Además de las entrevistas exclusivas y las anécdotas propias de Hispasec.

Incluye entrevistas exclusivas a los personajes relevantes de cada momento en el mundo de la seguridad: Bruce Schneier, Eugene Kaspersky, Cuartango, Mikel Urizarbarrena, Jorge Ramió, Johannes Ullrich... Además de noticias y anécdotas relevantes de cada año, fuera del ámbito de la seguridad informática. Por último, se han reproducido algunas de las mejores Una al día de todos los tiempos, las que mejor reflejan el estado de la seguridad en el momento en el que fueron redactadas.

Hispasec Sistemas
Seguridad y Tecnologías de la Información

ISBN 978-1-4092-4403-5

www.hispasec.com